

CREATORS  
OF  
CHANGE

CYBER RESILIENT CITIZENS



ADD US @YOUTHWORKDG



"The  
**BIGGEST**  
part of our  
digital transformation  
**IS CHANGING**  
the way we  
**THINK!"**

Simon Preston

# CONTENTS

## INTRODUCTION

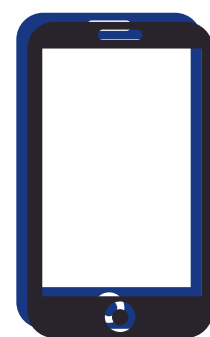
Introduction.....	05
Top Tips for Delivery.....	06
Group Agreement.....	07
Getting to Know One Another.....	08
Useful Information.....	10

## THE SESSIONS



### SESSION 1

Introduction to Cyber Resilience.  
Overview of the Programme.  
Digital Rights.



### SESSION 2

Introduction to Social Media.  
Social Media Safety & Security.  
Cyberbullying.



### SESSION 3

What is Cyber Crime?  
Scams 101!  
Catfishing & Hacking - an Introduction.



### SESSION 4

Digital Safety.  
2-Factor Authentication.  
Virus', Passwords & Privacy.



### SESSION 5

Creators of Change  
Let's make an inspiring internet!  
Awards.

## CONTEXT

Social media and technology are becoming bigger and bigger parts of our day to day lives, no more so than for young people who are growing up in an online world. Whilst most young people may be able to work technology better than adults, they lack the critical thinking, knowledge and media literacy skills which are key to being cyber resilient. In light of this, the Creators of Change - Cyber Resilient Citizens Programme was developed.

The programme was designed by a group of 10 young people from the Youth Enquiry Service in Dumfries, in a collaboration with youth groups from across Dumfries and Galloway. Funded through Youth Link Scotland's Cyber Resilience Badges and Resources Fund, it aims to support them learn important digital literacy skills in a relatable and engaging way helping them to build a safer, inspiring online world.

Creators of Change - Cyber Resilient Citizens has been designed for delivery with young people aged 11-14 in groups of 5 - 15.

# INTRODUCTION

---

# INTRODUCTION

In 2021, the Youth Enquiry Service Management Committee was awarded funding from Youth Link Scotland's Cyber Resilience Resource and Badge fund to develop a toolkit that aimed to equip young people to become cyber resilient and digitally literate.

The toolkit is targeted at young people aged 11-14, 14 - 18 and is suitable to be delivered across a range of settings and communities. It is designed to run for 5 Weeks, with each session running for approximately 2 Hours. This can be delivered as a stand alone project or built into ongoing work with pre-existing groups. It has been designed to enable the facilitator to tailor some of the activities to suit the needs and interests of the young people they are working with and the resources within their local community. The sessions have activities grouped in themes so each week's session should be delivered together, however the order in which these are delivered can be swapped around as Youth Worker see's fit.

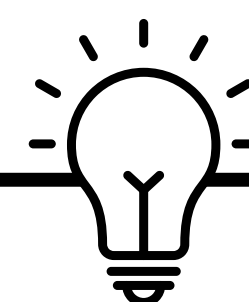
The activities in the sessions have been designed by young people using their own knowledge and activities they have previously taken part in. Where there are activities loosely based on another resource they are marked. The toolkit aims to use a game based learning approach to ensure that it is interactive, promoting the participation of young people throughout through teambuilding & games.

## TOOLKIT OUTCOMES

The Toolkit aims to:

- ✔ Develop young people's understanding of what cyber resilience means.

- ✔ Support young people to learn about and understand their Digital Rights.
- ✔ Ensure young people are equipped to keep themselves and others safe online - particularly on social media.
- ✔ Explore cyber crime, scams and hacking, supporting young people to be able to identify and report.
- ✔ Help young people build resilience and critical thinking skills in order to be alert when consuming online content.
- ✔ Support young people to recognize the power of the internet in shaping our attitudes towards other people.
- ✔ Help young people understand the difference between online hate speech and free speech.



## TOP TIPS

This toolkit is designed to be delivered alongside various forms of Accreditation.

The toolkit can be used as:

- A Youth Achievement Award Challenge (15 Hours).
- A Dynamic Youth Award.

Please remember to take photos and keep evidence to support these each week.

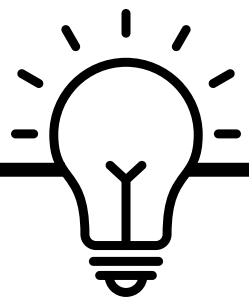
There will also be the opportunity for young people to undertake a Saltire Award Challenge later in the programme.



# TOP TIPS FOR DELIVERY

## FACILITATING

As the facilitator of this toolkit, your role is not to teach young people, rather to guide the young people through a process of self-education. The young people should come away from each session with a wider understanding of Activism, Leadership and Active Citizenship with increased knowledge on how their actions can help create change on a local, national and global level.



## TOP TIPS

There are five Top Tips for facilitating this toolkit:

1. **Plan.** Make sure your space is organised and ready to welcome young people. If there are any changes that need made to the room layout, plan time to organise these in advance.
2. **Be Prepared.** Ensure you are familiar with the session plan and any accompanying information. Ensure you have enough time to photocopy handouts, load up any videos or online content and gather resources as required.
3. **Create a supportive environment.** Develop the group agreement alongside young people that sets out their expectations for one another. Ensure that this is adhered to throughout and that young people are supported to participate.
4. **Active Listening.** Pay close attention to young people's body language, and non-verbal communication. Allow wait times for

4. young people to give responses in group discussions and prompt quieter young people to take part. Clarify information that may be unclear and ensure that complex terms are explained clearly.
5. **Don't be the expert.** Youth Work is built on the foundational principle that young people and youth workers are partners in the learning process. It is not essential for you to be an expert and if there is information you do not know, admit this and research it alongside young people, using it as an opportunity to learn together.

## DEFINING FEATURES OF YOUTH WORK

Youth Work has three essential and definitive features that are critical to the successful delivery of this toolkit. These are:

1. Young People choose to take part.
2. The work must build from where young people are at.
3. Youth Work recognises the young person and youth worker as partners in the learning process.

## FURTHER GUIDANCE

For further information or guidance on delivering Youth Work in Dumfries and Galloway please visit

<https://youthwork.dumgal.gov.uk/>

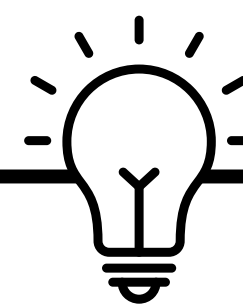
# GROUP AGREEMENT

Group agreements (not rules!) help to create safe and supportive environments that will enhance any group activity. They serve as a set of clear, co-created guidelines to help participants feel comfortable with each other in an atmosphere of safety, respect and trust. Everyone shares the responsibility for the experience and once developed, a group can regularly re-visit the agreements to see if they are still working and make changes if issues come up.

While agreements need to be generated by the participants themselves, the following outlines 10 common elements that promote a safe group environment:

- **Welcome** - participants will be welcoming of all new group members.
- **Confidentiality** - group agrees that what is said or done in the group, stays in the group and is not repeated outside. When discussing this it is important to ensure young people understand some information may need to be passed on under child protection if we feel they or someone else is at risk.
- **Put-ups, not put-downs** - aims to eliminate behaviours that may insult, make fun of, minimize, or attack other people in the group.
- **Right to pass** - supports people who don't want to talk in a group without asking them to explain themselves.
- **Personal accountability** - agrees that participants, will not take photos or videos during the group without permission from all group members and youth workers.

- **Respect** - includes the expectation that the group will respect one another even if they do not share the same beliefs, values and experiences.
- **Feelings happen** - An agreement that shows respect and opens the door for people to express feelings.
- **Give it a try** - trying out experiences and activities that are new and/or uncomfortable in a safe environment
- **Listen** - Listening to one another.
- **Show up and be present** - requires participants to set aside concerns and distractions and be as present as they are able.



## TOP TIP

If the group doesn't address these elements on their own, use this list as a discussion prompt during the development process.

Also, once young people have created their group agreement, type this up and give each young person a copy and ask them to sign it. It can also be helpful to print this on A3 and stick it up whenever the group are in as a reminder of their agreement.



# GETTING TO KNOW ONE ANOTHER

Depending on the setting in which you are delivering this toolkit, you may be working with a group of young people who don't really know one another. It is therefore beneficial to use Icebreakers to support young people to get to know one another better. Icebreakers play a significant role in helping break down the barriers that exist amongst groups of young people and can be an effective way to start a group work session.

There are lots of icebreakers out there and these can be looked up online or in other toolkits, however we have suggested a few to help get you started.

## NAME GAME (5 MINS)

This icebreaker aims to help young people get to know one another.

Sitting or standing in a circle, ask young people to take it in turns introducing themselves by their first name and an animal that begins with the same letter as their name. For example, I am Georgia and I like Giraffes.

You can then repeat this exercise asking young people to name something to do with climate change a category that the young people choose themselves.

If you have the time, and if a group doesn't know each other well, then you could ask them to try and remember the names and descriptions of everyone else.

## WHO AM I? (20 MINS)

This icebreaker aims to help young people begin to develop relationships with one another.

Prepare a post it note for each of the young people and write on it the name of a famous individual that is in some way related to Activism i.e. Greta Thunberg.

On arrival, stick the post it note on the back of each young person, who must then ask questions in order to find out their identity. Each question can only be answered with yes or no i.e. Am I a human? Yes.

Once young people have discovered who they are, ask them to think about what all these people have in common - Activism. This will help link into the start of the session.

## CANDY INTRODUCTIONS (10 MINS)

This icebreaker aims to help young people discover facts about one another and build relationships. For this, you will need a bag of multi-coloured sweets. Ask young people to take 3 sweets from the bag (each a different colour) but ask them not to eat these yet.

Once everyone has a sweet, assign an attribute to each colour i.e. red - favourite hobby. Go around the group and ask each person to answer the question attached to their coloured sweet. Then eat them!



## RESPECT (20 MINS)

This icebreaker aims to encourage young people to get to know one another and establish respect within the group.

Ask everyone in the room to find someone who they do not know well and ask them to introduce themselves.

Ask each pair to spend 5-10 minutes exploring what it means for them to show and be shown respect.

After the allotted time, ask everyone to come back together and open a discussion - what did people come up with?

The point of this exercise is to encourage young people to learn from their differences and to understand one another better.

## MY NAME... (10 MINS)

This icebreaker aims to help young people begin to get to know one another.

Split the group into pairs. Ensure these are pairs that have not worked together before. Ask each pair to come up with words that describe the other person using the letters in their first name. For example, Lyndsay could stand for, "Loud, Young, Nerdy, Dreamer, Strong, Adventurous, Yearning."

Once all the pairs have come up with their names, bring the group back together and ask each pair to share their names and what each letter stands for.

## MAROONED (10 MINS)

This icebreaker aims to encourage critical thinking, communication and teamworking.

Ask the group to separate into smaller groups of no more than 4 people. Ask them:

"If you were marooned on a desert island, what 3 items would you bring with you?"

Allow each individual to choose 3 items and ask the groups to then present the back to the group.

Explain to the group that unfortunately, they are only able to now take 3 items between the team. Ask them to discuss which of their individual items they would be willing to give up. Encourage them to think practically about survival instead of sentimentally.

Bring the groups back together to ask them to discuss what they came up with and how they made their decisions on what items to take.

## HUMAN KNOT (10 MINS)

Ask the group to stand very close together. Ask them to reach out their arms so that all of their hands are jumbled and intertwined.

Ask them to grab one hand for each of their hands, but not the one of the person's next to them. Now they are a human knot and must use teamwork and communication skills to untangle themselves into one circle without letting go of their hands.

## NUMBERS (15 MINS)

Ask young people to walk around and mingle in the space. Randomly call out a number. Young people must try and get into groups of that number. Any that do not end up in a group are out of the game. Repeat this until you have a winner.

# USEFUL INFORMATION

The following websites are for local, national and international agencies who can offer more information and support when delivering activism themed activities with young people.

## YOUTH LINK SCOTLAND

Youth Link Scotland is the national agency for Youth Work in Scotland. As part of their remit, they have worked to develop a Digital Youth Work Resource Library that aims to equip Youth Workers with the tools and resources they need to deliver Digital Youth Work and explore cyber resilience topics with young people.

<https://www.youthlinkscotland.org/develop/developing-knowledge/digital-youth-work/>



## THINK U KNOW (CEOP)

CEOP is a command of the National Crime Agency and is dedicated to using education to prevent online and offline Child Sexual Exploitation (CSE). They have a plethora of resources available to help professionals deliver workshops around cyber resilience and online safety including toolkits, session plans and presentations.

<https://www.thinkuknow.co.uk/professionals/resources/>



## CYBER SECURITY CHALLENGE UK

The Cyber Security Challenge UK is an organization aiming to support young people into the Cyber Security industry. They provide information, advice and resources themed around cyber resilience and digital literacy with various resources available to support the delivery of this work.

<https://cybersecuritychallenge.org.uk>



## YOUTHWORK DG DIGITAL YOUTH WORK PADLET

Youth Work Dumfries and Galloway's Digital Youth Work Padlet is a collection of resources that aim to equip youth workers to deliver digital youth work. It contains information on digital literacy, safeguarding / child protection, cyber resilience, games and much more!

[https://padlet.com/youth\\_work\\_dg/digitalyouthwork](https://padlet.com/youth_work_dg/digitalyouthwork)



# DIGITAL RIGHTS

---





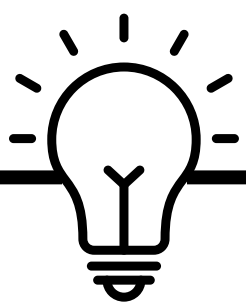
# WEEK 1

## INTRODUCTION

Session 1 of the Toolkit aims to introduce young people to Cyber Resilience, give them an overview of the Programme and explore with them their Digital Rights.

## SESSION OVERVIEW

- Introduction (**5 Mins**)
- Group Chat / Group Agreement (**10 Mins**)
- Word Association (**10 Mins**)
- Agree / Disagree (**15 Mins**)
- Scavenger Hunt (**20 Mins**)
- Break (**5 Mins**)
- Digital Rights (Young Scot) (**15 Mins**)
- Getting to a Million... (CEOP) (**30 Mins**) (**14-18 Only**)
- Group Discussion (**10 Mins**)



### TOP TIP

The whole session should last for 2 hours. If you are short on time, focus on the group agreement, Digital Rights games and group discussion.

## RESOURCES

- ➔ Flipchart Paper.
- ➔ Marker Pens.
- ➔ Handout 1 - Group Chat.
- ➔ Handout 2 - Word Association.
- ➔ Handout 3 - Agree / Disagree.
- ➔ Handout 4 - Scavenger Hunt.
- ➔ Handout 5 - Getting to a Million.
- ➔ Access to a Laptop or Device with an Internet Connection.

## LEARNING OUTCOMES

Young People will:

- ✔ Know about and be able to apply the 5 Digital Rights to their Online Activities.
- ✔ Consider appropriate peer-to-peer interactions online.

## DELIVERY NOTES

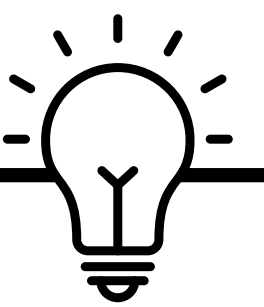
Prior to delivering the session, Youth Workers should:

- Read through the session plan, key terms and familiarize themselves with the resources.
- Prepare the Scavenger Hunt by placing clues around the space.

## OPENING ACTIVITIES

### Programme Introduction (5 Mins)

Explain to young people that the purpose of this programme is to support them to develop their Cyber Resilience and Digital Literacy Skills.



### TOP TIP

If young people aren't familiar with the terms digital literacy or cyber resilience, use the Key Terms listed below to help explain these to them.

Explain that they will learn about social media, cyber crime, virus' and password protection before working together to brainstorm ways in which they can work to combat some of the issues young people face online.

## KEY TERMS

**Digital Literacy** - Digital Literacy is defined as having the basic digital skills you need to do your jobs, live your life and confidently, using different digital services. (Scottish Qualifications Authority, 2020)

**Cyber Resilience** - An individual's ability to use technology securely, and to respond to and prevent cyber crime. (Scottish Government, 2021)

## OPENING ACTIVITIES

### Group Chat / Agreement (10 Mins)

The aim of the Group Chat / Agreement is to enable young people to feel comfortable and able to openly discuss the issues raised as part of this programme.

Go around the room and ask every young person to say their name, their favorite social media platform and if they were to be a piece of technology, what they would be and why.

Using flipchart paper, ask each young person to suggest a value that they think they need in the group for everyone to feel safe. Write these on the flipchart using Page 7 - Group Agreement to help.

Ask young people to rank the values listed from the most important to the least important. Reinforce, that all of them will form part of the group agreement, but that they need to decide which 3 are vital.

Ask young people to do the same thing again, but this time, rank them in order for online communication. What, if anything changed? If it did, why?

Was there anything that was added? Why?

Using the two sets of ranked values, ask young people to decide on which 3 are the most important for both online and offline communicating. Ask them to write these down on Handout 1 - Group Chat in the "Key Message Boxes."

Get young people to think about 1 sentence that would describe how to effectively communicate online. Ask them to write this in the Laptop on their Handout.

Finally, ask young people to sign the group agreement. (This will be covered at the start of every session.)

## DEVELOPMENT

### Word Association (10 Mins)

The aim of Word Association is to find out where young people are at with their knowledge of digital literacy and cyber resilience.

Start the game by reading out one of the words on Handout 2 - Word Association. Once you have read out the word, go around the room asking each young person to say the first thing that pops into their mind when they hear that word. Repeat this for every word.

This will give you an insight into young people's understanding of digital, in particular where they are at with some of the topics that are included in the programme.

Finish by asking young people to suggest a word to start the game and repeat for each person.



### Agree / Disagree (15 Mins)

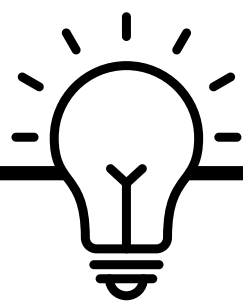
This activity aims to introduce young people to the topic of today's session - Digital Rights and gauge their understanding of the topic.

Separate the room into 3 sections - Agree / Disagree and Don't Know.

Read out the statements listed on Handout 3 and ask young people to answer by moving to an area of the room. Afterwards, ask young people to feedback why they gave the answer they did.

Facilitate discussions between young people around their answers, encouraging opposing viewpoints.

### Scavenger Hunt (20 Mins)

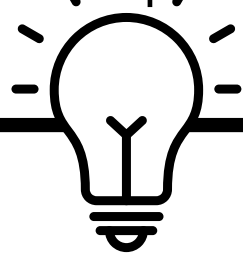


#### TOP TIP

This activity needs to be set up prior to young people arriving during prep time.

The aim of this activity is to support young people to think about how diverse digital technology is, and give them the opportunity to identify and learn about their Digital Rights.

Using Handout 4 - cut out the 15 riddles and clues and stick them up around your space in the order listed.



#### TOP TIP

Make sure you have enough photocopies of the clues for the size of your group i.e. if you have 20 young people, and split them into 5 groups, you will need 5 copies of the clues as each group needs their own set.

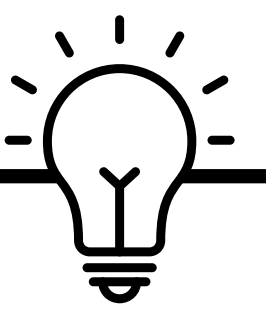
Split young people into groups of 4 or 5 and explain to them that they are going to be taking part in a scavenger hunt themed around digital rights.

Explain that at each location they will find:

- A Riddle - which will guide them to their next location.
- A Clue - which they need to take 1 of!

Reiterate to young people that the only thing they are taking from each location is the clue, not the riddle.

Start each of the groups off, reading out the first riddle.



#### TOP TIP

Depending on the number of groups, you might want to start them off at intervals i.e. start 1 group at riddle 1, 1 group at riddle 6, 1 group at riddle 10 etc.

Guide young people through the scavenger hunt, providing assistance if and when needed.

Once complete, explain to young people that the clues they have gathered make up their 5 Digital Rights (Young Scot) and that their task is to piece together the clues into 5 sentences which make up their rights.

Once all groups have piece together what they think their rights are - reveal the answers, taking time to explain to young people what each right means (Handout 4).

Take a note of the winners from the group, and arrange to get them a prize for next weeks session.



### **Break (5 Mins)**

Give young people a 5 minute break. Offer refreshments and allow them time to process what's been discussed so far.

### **Digital Rights (Young Scot) (15 Mins)**

Split young people into 5 groups and give each group a different Digital Right:

- The right to know.
- The right to remove.
- The right to safety and support.
- The right to informed and conscious choices.
- The right to digital literacy.

Task each group with creating a short game, a poster, a video or social media post that explains their given digital right to other young people. Encourage them to be as creative as possible!

### **Getting to a Million (CEOP) (30 Mins) (14 - 18 Only)**

*\*Please note, this activity requires an internet connection.*

Start the activity by splitting young people into 2 groups. Task each group to come up with an idea for a Tik Tok video that they think will get them 1 Million views.

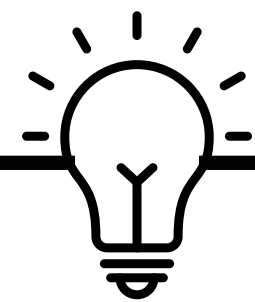
Encourage them to think outside the box, getting creative and using whatever resources they have at hand. If young people are finding this difficult, allow them access to a phone or device to search for ideas.

Allow 10 minutes for young people to brainstorm their ideas, before bringing them back together and asking them to present these to one another. Then, ask each group to vote on which idea they think would be most likely to get them 1 Million Views.

Next, ask young people to stand in a Line at one side of the room. Explain that you are going to read out a series of statements and if it is something they would consider doing, would do or have done, they need to take a step forward.

Read out the statements (Handout 5) and once you have read them all, ask young people to have a look around at where they are all standing, compared to where they were at previously.

Bring young people back together and encourage them to discuss how they found the activity.



### **TOP TIP**

This activity may bring up some powerful emotions for young people, so it is key that you remind the group of their group agreement.

Explain to young people that some of the activities listed would infringe on other people's digital rights. Rights come with responsibilities and it is everyone's responsibility to protect one another's rights.

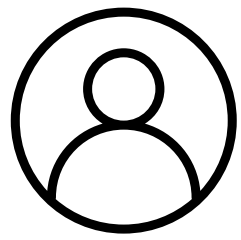
Using Handout 5 - The Law, go on to explain the legalities of information sharing online, taking time to talk in particular, about the sending, receiving and sharing of nude pictures.

## **REFLECTION**

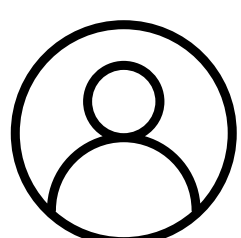
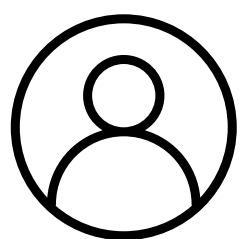
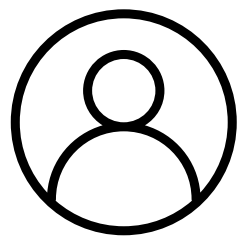
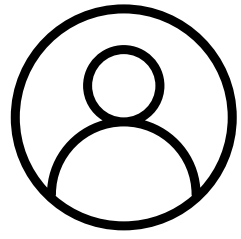
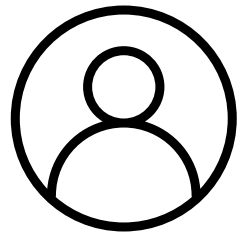
### **Group Discussion (10 Mins)**

Give young people 10 minutes at the end of the session to discuss what they have learned.

# HANDOUT 1 GROUP CHAT



GROUP MEMBERS:



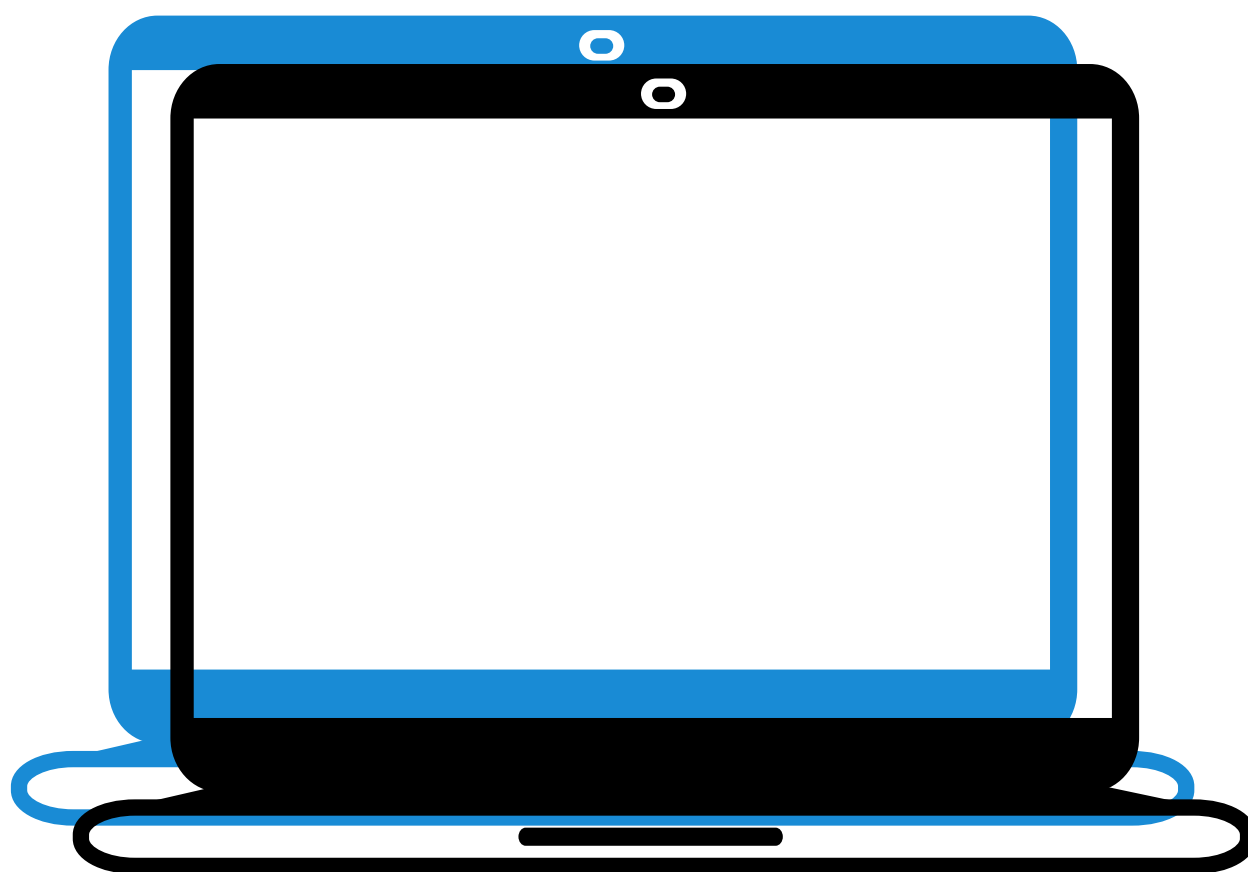
IN THE MESSAGES BELOW  
WRITE DOWN WHAT YOUR  
GROUP DECIDES ARE THE KEY  
MESSAGES OF YOUR CHAT.

KEY MESSAGE 1:

KEY MESSAGE 2:

KEY MESSAGE 3:

USE THE LAPTOP TO WRITE DOWN YOUR  
GOLDEN RULE FOR COMMUNICATING ONLINE:



SIGNATURE:

WHICH OF THESE ARE THE MOST IMPORTANT PART OF A GROUP CHAT?



OPEN

RESPECTFUL OF OTHERS



CONFIDENTIALITY



QUESTIONING



NON JUDGEMENTAL



LISTENING



# HANDOUT 2 WORD ASSOCIATION

- Digital
- Media
- Virtual
- Fake News
- CEOP
- Cyber
- Virus
- Hacking
- Cyber Crime
- Report
- Literacy
- Hate Speech
- Catfishing
- Social Media
- Apps
- Resilience
- Protection
- Electronic
- Gaming
- Download
- Online
- Password
- Mobile
- Chat Room
- Bias
- Rights
- Secure
- Device
- Responsibilities
- Filters

# HANDOUT 3 AGREE / DISAGREE

- I can do whatever I want online and I won't get into trouble because it is my online identity talking, not me.
- I can post whatever I want and I don't need anyone's permission.
- If I post a picture online, it is easy for me to remove it.
- I can say whatever I like online as there are no repercussions.
- I can screenshot whatever I like and share it with whomever I like.
- Age restrictions on social media / apps don't matter.
- I can share any personal information about myself online and it is perfectly safe.
- I don't need to worry about privacy settings as they aren't there for any good reason.
- I can lie about who I am online and no one will find out.
- I can use the same password for everything.

# HANDOUT 4 SCAVENGER HUNT RIDDLES

1. I can take you to places you've never seen, but first, type your password in on my screen.

2. You push my buttons and use me to call. I can reach very far, but I'm not that tall.

3. I have no fingers but own a ring. When I receive information, I often go "Ping!"

4. You can feed me, I like to eat paper. I have a tray but I'm not a waiter.

5. You often play with me, on games with no referee.

6. In many rooms, I can be seen. You watch things on my widescreen.

7. I have no voice and yet I speak. Don't turn me up too high or else I'll squeak.

8. I help you play games by giving you control - I can even help when you want to scroll.



9. I have many keys but can't open a door. I have space that you can't explore.
10. I don't go anywhere without you dragging me along. Attached to a computer is where I belong.
11. I make your phone work. Next to a plug is where I lurk.
12. I am only online and awake ALL the time. I help you meet new people but am responsible for your screentime.
13. If you plug me in, music is all you'll hear. I fit neatly inside your ear.
14. If you see something is wrong, use me you must. I make the internet safer, in that you can trust!
15. I wear a blue T-Shirt and am always around. In your local community is where I'll be found.

## SCAVENGER HUNT RIDDLE ANSWERS

1.Computer	6.TV	11.Charing Cable
2.Landline Phone	7.Speaker	12.Social Media
3.Mobile Phone	8.Games Console Controller	13.Headphones
4.Printer	9.Keyboard	14.Report Button
5.Games Console	10.Computer Mouse	15.Youth Worker

## SCAVENGER HUNT CLUES

Informed.	The Right to...	Remove.
The Right to...	Choices.	And Conscious.
Know.	The Right to...	Literacy.
And.	The Right to...	Digital.
Safety.	The Right to...	Support.

# HANDOUT 4 DIGITAL RIGHTS

"Sometimes I regret what I post online and wish there was some easy way to make it disappear."

THE RIGHT TO  
**remove**



THE RIGHT TO  
**know**

"We should know who is holding and profiting from our information."



"There is too much emphasis on what is illegal and not enough about what is unpleasant or distressing."

THE RIGHT TO  
**Safety & support**



THE RIGHT TO  
**informed and conscious choices**

"Unless we understand the technologies we use daily we can't control how they make us behave."

"We need to be taught the skills to use digital technologies effectively."

THE RIGHT TO  
**digital literacy**



# HANDOUT 5 STATEMENTS

What would you do, to get 1 Million Views?

Would you:

- Make or Share a video pulling a prank on someone.
- **Make or Share an image threatening someone.**
- Make or Share a video of an animal.
- **Make or Share a video containing someone's personal information.**
- **Make or Share a video or image containing nudity.**
- Make or Share a video of you or your friends.
- **Make or Share an image making fun of someone because of their age, gender, sexual orientation, religion, disability or race.**
- Share a video that has gone viral.
- **Make or Share a video of violence.**
- Make or Share a video of your family.

# HANDOUT 5 THE LAW

It is a criminal offence and therefore illegal:

- To possess, distribute, show and make indecent images of children. A child in this context is defined as anyone under the age of 18.
- To discriminate against or target someone which is motivated (wholly or partly) by malice or ill will towards a social group (age, gender, sexual orientation, religion, disability or race).
- Under the Serious Crime Act, to make or share videos that incite violence.
- To threaten to kill, harm or to commit an offence against a person, group of people or organization. This can be prosecuted under the Malicious Communication Act 1988 and the Communications Act 2003.
- To obtain or disclose personal data without consent.





**SOCIAL MEDIA**



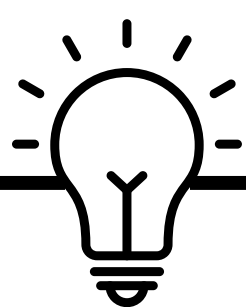
# SESSION 2

## INTRODUCTION

Session 2 of the Toolkit aims to introduce young people to Social Media, Social Media Safety & Cyber Bullying.

## SESSION OVERVIEW

- Introduction (**5 Mins**)
- What am I? Social Media Edition (**20 Mins**)
- What is social media? (**10 Mins**)
- Search Bar (**20 Mins**)
- Share / Don't Share (**15 Mins**)
- Investigation Games (**35 Mins**)
- Cyber Bullying (Citizenship Foundation) (**15 Mins**)



### TOP TIP

The whole session should last for 2 hours. If you are short on time, focus on Share / Don't Share, Cyber Bullying & Keeping Safe.

## RESOURCES

- ➔ Post it Notes.
- ➔ Pens.
- ➔ Flipchart Paper.
- ➔ Handout 6 - What am I? Questions.
- ➔ Handout 7 - Search Bar.
- ➔ Handout 8 - Share / Don't Share
- ➔ Statements.
- ➔ Handout 9 - Cyberbullying.

## LEARNING OUTCOMES

Young People will:

- ✔ Understand why some data should be kept private when setting up online profiles.

- ✔ Know how to react to cyberbullying, grooming and other online exploitation.

## DELIVERY NOTES

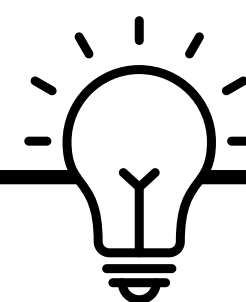
Prior to delivering the session, Youth Workers should:

- Read through the session plan, key terms and familiarize themselves with the resources.
- Prepare the What am I? Post it Notes.

## OPENING ACTIVITIES

### Introduction (5 Mins)

Explain to young people that the aim of today's session is to explore Social Media, Cyber-bullying and keeping safe when using social networking.



### TOP TIP

If young people aren't familiar with the terms social networking or cyberbullying, use the Key Terms listed below to help explain these to them.

## KEY TERMS

**Social Networking** - the use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own. (Oxford English Dictionary).

**Cyberbullying** - the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. (Oxford English Dictionary)

## OPENING ACTIVITES

### **What am I? Social Media Edition (20 Mins)**

Start this activity by writing out different social media platforms on to post it notes - 1 per post it. Some examples could be Facebook, Snapchat, Tik Tok, Pinterest, YouTube etc.

As young people come in, give them each a post it note and ask them to stick this to their forehead without looking at it.

Then, using Handout 6, ask young people to ask yes or no questions and try to find out what social media platform they are. The rest of the group should answer the questions until they are finally able to guess who or what they are.

This should repeat until everyone has discovered which platform they are.

## DEVELOPMENT

### **What is Social Media? (10 Mins)**

It is important before you move any further through the programme, that young people all have the same basic understanding of social media. Through this activity, young people who are more familiar with different online platforms, will be able to act as peer educators for other members of the group.

Give each young person a copy of Handout 7. In groups of 2 or 3 ask young people to come up with a definition of social media.

Ask groups to feedback what they came up with. Give young people the 'dictionary definition' of social media (below) and

discuss. Do they agree / disagree with this?

As a group, guide young people to come up with their groups definition of social media. Ask young people to write this in the space provided.

### **"Websites and Applications that enable users to create and share content or to participate in social networking"**

Ask young people to spend time thinking about what social media is for them. What does it help them do? Why do they use it, before bringing them together to discuss.

### **Search Bar (20 Mins)**

All young people will have had different experiences of social media and their engagement with it will have been different. It is important that we know where they are at and how they feel about it, so that we are able to provide them with a tailored programme. The Search Bar activity, aims to identify where young people are at.

Ask young people to complete the rest of the Search Bar page, starting with writing down all the types of social media they can think of. If they are struggling, prompt them to consider other online activities such as gaming, blogs or web-chat. For an exhaustive list, google social media sites. This will give you an indication of what platforms young people are most comfortable with (their top 3 will be the ones they use the most) so, moving forward, examples can be tailored to these to make it most relevant to young people.



Next, ask young people to think about some of the reasons that you might use the internet. This can be done on flip-chart in a group setting or written individually. Again, the first 3 young people come up with are likely to be the reasons that they use the internet, so bear this in mind moving forward.

Lastly, ask young people to circle the words they associate with social media. The words have been specifically chosen to give you an indication of whether or not young people are comfortable online. If they are not, they will have circled words such as scared, fake, overwhelming. If they are comfortable they may have circled, friends, fun or positive.

### **Share / Don't Share (15 Mins)**

Following on from the last activity, this activity aims to explore with young people what information and content is appropriate for them to share online.

Give each young person a set of the Share Don't Share Cards (from Handout 8), and ask them to sort it into two piles. 1, of which is appropriate to share, and the other of which they shouldn't share.

Ask young people to give 1 example of what they put in each category and why.

Explain that information such as their address, phone number and school they attend, is personal and private, so should not be posted online and should be in the Don't Share category as this puts them at risk. It is important to also highlight here that they should not post images or videos of themselves or others while they are wearing their school uniform as it is easy for people to then identify their school from this.

It is important that young people know what they can share, so go over these also, and give an example of why these are appropriate i.e. sharing a photo from a trip when they are home, does not put them at risk as they are no longer there and also are not sharing personal details.

Encourage young people to always think about this before they post information online. Explain the SMART Anagram (listed below) and explain that the most important letter of these is T - Tell. Encourage young that if at any point they are worried about ANYTHING they see online, they should tell a trusted adult, youth worker, teacher or report it to the police.

**S - SAFE - Do not share personal information, email, phone numbers, addresses and passwords.**

**M - MEETING - Never meet someone you have only met online.**

**A - ACCEPTING - Do not open emails, texts and files from an unknown source, this can lead to virus' or scams.**

**R - RELIABLE - Information on the internet is not always true. People post false details.**

**T - TELL - Inform a parent or carer or a trusted adult if anything online makes you feel uncomfortable or worried.**

### **Investigation Games (30 Mins)**

The aim of this activity is to help young people notice some of the indicators of Fake Social Media Accounts.

Split young people into groups of 5 or 6. Give each group 10 minutes to design a fake social media profile / account. They should come up with the following:

- Full Name
- Profile Name i.e. @\_\_\_\_\_
- Age
- Profile Picture
- Cover Photo
- About Information (Current Town / City, Workplace, Education, Home Town, Relationship Status).
- Posts - What would this person post on their feed? What type of images / videos might you expect to see?

Once young people have finished their Fake Account, ask them to swap with another group. Give each group 10 minutes to identify what about the account makes it fake or can indicate it is fake. Ask them to circle the areas that they think make it fake and explain why.

When all young people have finished, bring them back together. Ask them to swap back their Fake Accounts and present these to everyone revealing why they chose to make it the way they had.

Then, once all groups have presented ask them to discuss how easy or not they think it is to identify fake accounts online. Use the following questions to help prompt discussions.

## FOR DISCUSSION

- Do you think there are fake accounts on social media?
- How easy or difficult is it to identify these accounts?
- What can indicate that an account is fake?

Finally, explain to young people these 5 top tips to identify a fake account online. Allow young people to share their thoughts on these tips, and if they have any of their own add these in. It is important to explain to young people that these are only a guide and tips - some fake accounts will go to extreme lengths to look real hence why you should only add people you know.

1. Profile Picture - if their profile picture is blank, an avatar or a cartoon this can be an indication the account is not real.
2. Posts - if their feed is filled only with shares of other people's posts or of only one topic / opinion that can indicate that it has not been created by a person.
3. Friends List - check their friends list. If they don't have any friends or followers and don't follow any pages this can suggest the account is fake.
4. Timeline - if their biography says they are from the UK but all their posts are from another country or seem to have no origin / location this can indicate the account is fake.
5. Interaction - if the account does not interact with other users and only posts, but doesn't like or comment this can indicate it is fake.

## Cyberbullying (Citizenship Foundation) (15 Mins)

This activity has been designed to introduce young people to what might be considered cyberbullying and the potential impact it may have on those involved. Split students into pairs and give each pair a copy of Handout 9 - What is Cyberbullying? Give the pairs 5 minutes to discuss the questions on the worksheet and note down their ideas.



Once the pairs have had time to note down their ideas bring them back together and discuss each question. Use the supporting information below to help with this.

### **What is cyberbullying?**

The Crown Prosecution Service (CPS) guidelines (Oct 2016) refer to cyberstalking rather than cyberbullying. There is no legal definition for either cyberstalking or cyberbullying. However, the following definition is based on the CPS guidelines: "The use of electronic communications to bully a person, typically by sending messages that intimidate, threaten, harass or relate to stalking another individual." It is important to remember that these things can be prosecuted under the Malicious Communications Act 1998 and the Communications Act 2003.

### **What forms can cyberbullying take?**

Cyberbullying is bullying that takes place using electronic technology; this includes devices and equipment such as mobile phones, computers and tablets. The CPS guidelines outline the following activities: Sending threatening or obscene emails or texts, spamming - sending multiple junk emails, live chat harassment or 'flaming' (a form of online verbal abuse), 'baiting' or humiliating peers online by labelling them as sexually promiscuous, leaving improper messages on online forums, posting 'photoshopped' images of people on social media platforms, hacking into social media accounts, sending electronic viruses, cyber identity theft.

### **Why do you think cyberbullying takes place?**

This is a complex issue, cyberbullying can take place for a variety of reasons.

Often people who choose to get involved with cyberbullying will do it because they think that they are more likely to get away with it. They might not realise how upsetting what they are doing is as they cannot see how their target reacts. They might also think less about the consequences of their actions because they are behind a device and therefore their identity can be easily hidden.

### **What impact can cyberbullying have on someone's life?**

People will react differently depending on their current situation and the extent of the bullying that is taking place. As with all types of bullying it can be extremely upsetting and can lead to poor self-esteem and mental health.

Finish the session by reminding young people of SMART and that if they need to speak to anyone about anything they have been discussing, they can.

**S - SAFE - Do not share personal information, email, phone numbers, addresses and passwords.**

**M - MEETING - Never meet someone you have only met online.**

**A - ACCEPTING - Do not open emails, texts and files from an unknown source, this can lead to virus' or scams.**

**R - RELIABLE - Information on the internet is not always true. People post false details.**

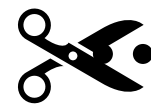
**T - TELL - Inform a parent or carer or a trusted adult if anything online makes you feel uncomfortable or worried.**



# HANDOUT 6 WHAT AM I QUESTIONS!

- 1. Can I share videos?
- 2. Can I share links?
- 3. Does my icon contain a letter?
- 4. Can I post pictures?
- 5. Can I post stories?
- 6. Is my main feature...?
- 7. Can I video chat through this?
- 8. Do I help you keep in touch with people you know?
- 9. Do I help you make new friends?
- 10. Is my logo an object?
- 11. Does this platform inspire people?
- 12. Do I have ads?
- 13. Can I be used casually?
- 14. Am I for over 16's only?
- 15. Do I allow live videos?
- 16. Can I get verified on here?
- 17. Can I dislike on this platform?
- 18. Did I exist before 2010?
- 19. Is it for professional use?
- 20. Did I have another name?

Please cut here



# HANDOUT 7 SEARCH BAR

WRITE DOWN ALL THE TYPES OF SOCIAL MEDIA YOU CAN THINK OF.

WHAT IS SOCIAL MEDIA? WRITE YOUR ANSWERS IN THE MESSAGE.

WHAT ARE SOME OF THE REASONS YOU MAY USE SOCIAL MEDIA OR THE INTERNET. WRITE THEM BELOW.

WHICH OF THESE WORDS DO YOU ASSOCIATE WITH SOCIAL MEDIA AND THE INTERNET? CIRCLE ALL THAT APPLY.

FRIENDS

REALISTIC

CONNECTIONS

SCARED

FUN

INFORMATIVE

FAKE

MEDIA

VIDEOS

PRIVATE

INTERESTING

POSSITIVE

APPS

OVERWHELMING

GAMES

PHOTOS

ONLINE

NEW PEOPLE

UNKNOWN

COMMUNICATION

# HANDOUT 8 SHARE / DON'T SHARE

Information from Organisations.	Personal Information about friends or family.
Photos or selfies.	My date of birth.
A review of an item that I have bought.	Where I go to school.
A petition or campaign I support.	My password for social media.
Good news / something I am proud of.	My bank account details.
My favourite book.	My email address.
What box set / series I am currently watching.	My schedule or plan for the week.
My favourite band / music.	My Phone Number.
A photo of me and my friends.	My Home Address or a Geo Tag when I post a photo from home.
<b>SHARE</b>	<b>DON'T SHARE</b>

# HANDOUT 9 CYBERBULLYING

WHAT IS CYBERBULLYING?

WHAT FORMS CAN CYBERBULLYING TAKE?

WHY DO YOU THINK CYBERBULLYING TAKES PLACE?

WHAT IMPACT CAN CYBERBULLYING HAVE ON THE LIVES OF THOSE INVOLVED?



# CYBER CRIME

---

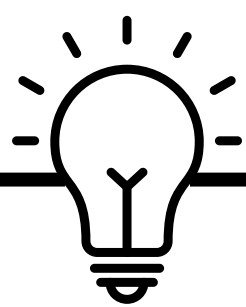
# SESSION 3

## INTRODUCTION

Session 3 is designed to introduce young people to Cyber Crimes and support them to be able to identify these in future.

## SESSION OVERVIEW

- True or False - Facts You Know! (**Be Internet Citizens**) (15 Mins)
- Introduction to Cyber Crime (5 Mins)
- Spot the Scam (20 Mins)
- Speed Friending & Catfishing (CEOP)(40 Mins)
- Captcha! (Cyber Security Challenge UK) (20 Mins)



### TOP TIP

The whole session should last for 2 hours. If you are short on time, focus on Speed Friending & Catfishing, Hacking & Capatcha!

## RESOURCES

- ➔ Handout 10 - True or False.
- ➔ Flipchart Paper & Pens.
- ➔ Handout 11 - Spot the Scam.
- ➔ Handout 12 - Speed Friending.
- ➔ Device with an internet connection.

## LEARNING OUTCOMES

Young People will:

- ✔ Learn to identify cyber crimes including scams, phishing and catfishing.
- ✔ Develop their understanding of online security measures such as Captcha.

- ✔ Know how to report cybercrime and how to block people from social media.

## DELIVERY NOTES

Prior to delivering the session, Youth Workers should:

- Read through the session plan, key terms and familiarize themselves with the resources.
- Check the internet connection is working and load Police website.

## OPENING ACTIVITIES

### True or False - Facts You Know! (Be Internet Citizens) (15 Mins)

It is important to identify, before moving forward, exactly what young people do and don't know so that you can fill gaps in their knowledge through the session.

Young People get the majority of their information online and more and more this information is inaccurate. made up or completely false. This activity aims to provoke discussions, and help young people develop their critical thinking skills and ultimately identify what is and is not false online when looking for information.

Ask young people to create a true, false and not sure sign on flipchart paper. Explain that you will be reading out a list of statements (Handout 10) about internet safety and fake news and they need to decide if they believe it is true, false or they are not sure.

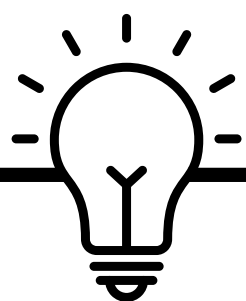
Work through each of the questions one by one, asking young people why they think something is true or false.

Don't reveal the answers to the questions until you have been through all of them.

Show young people the answers. Ask them if anything surprised them. If so, what? Why did they find it surprising? Is there anything they have learned that they did not know before?

### Introduction to Cyber Crime (5 Mins)

Take time to introduce the topic of today's session. Explain to young people that all of the activities they will take part in are in some way related to Cyber Crime.



#### TOP TIP

If you have time, take 5 minutes to ask young people what they think cyber crime is. Can they give any examples? Use the definitions below to help with this.

## KEY TERMS

**Cyber Crime** - criminal activities carried out by means of computers or the internet. (Oxford English Dictionary)

**Catfishing** - the process of luring someone into a relationship by means of a fictional online persona. (Oxford English Dictionary)

**Hacking** - the gaining of unauthorized access to data in a system or computer. (Oxford English Dictionary)

**Phishing** - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. (Oxford English Dictionary)

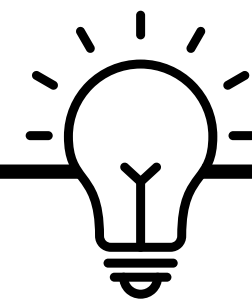
**Scams** - a dishonest scheme; a fraud. (Oxford English Dictionary)

**Captcha** - Completely Automated Public Turing Test To Tell Computers and Humans Apart. It is a program that challenge's a user's response to tell if they are a human or a computer. (Cyber Security Challenge)

## DEVELOPMENT

### Spot the Scam (20 Mins)

Split young people into 5 groups and give each group a Scam Picture (Handout 11). Give each group 10 minutes to identify the things in their image that help them to identify that it is a scam.



#### TOP TIP

If young people finish this early, ask them to identify what type of scam this might be and how it might impact the person involved.

Once young people have done this, bring them back together as a group and ask someone from each group to present their scam and what helped them to tell it was a scam.

Go over the answers (Handout 11) and reinforce the Tips to avoid scams.

Then, using the Police Scotland website [www.scotland.police.uk](http://www.scotland.police.uk) explain to young people how they can report a cyber crime. Using the information on the website, explain what they will ask, and what information young people might need to give when phoning 101 to report a Cybercrime.



Finally, using the guides below, ensure young people know how to Block someone on social media or report suspicious behavior. Explain to young people that these guides are based on accessing social media from a phone, and that if they are accessing on a different type of device where things are might not be exactly the same, but will be similar.

**Facebook** – To Block someone, click on their profile. Next to the message button, click on the 3 small dots. Select Block. A pop up will appear. Select Block again. To report something either click the 3 dots on the post or if it is a comment, click and hold, and select report comment. Complete the form that appears and you will have reported the comment.

**Instagram** – To Block someone, click on their profile. Next to the message button, click on the 3 small dots. Select Block. A pop up will appear. Select Block again. To report something click the 3 dots on the post and select report comment. Complete the form that appears and you will have reported it.

**Twitter** – To Block someone, click on their profile. Next to the message button, click on the 3 small dots. Select Block. A pop up will appear. Select Block again. To report something click the 3 dots on the tweet and select report. Complete the form that appears and you will have reported it. This is the same for all tweets / comments.

**Tik Tok** – To Block someone, click on their profile. Next to the message button, click on the 3 small dots. Select Block. A pop up will appear. Select Block again.

To report something click and hold, and select report. Complete the form that appears and you will have reported the comment or video.

If young people regularly use other social media platforms that are not listed, encourage them to create their own guide by researching how to report and block on that platform that they can then share with others.

### **Speed Friending & Catfishing (CEOP) (40 Mins)**

Young people may come into contact with people who are not what they seem when they are online. This activity uses role play to explore the nature of 'friendships' on social media and aims to support young people to identify risk, develop their critical thinking skills and develop their confidence in safely socializing online.

Ask young people – What qualities do you look for in a friend? Identify key words and write these down.

Ask young people – What qualities do you look for in an online friend? Make a new list with key words.

Compare the two lists and discuss. What is similar, or the same? Is anything different? Why is this? Prompt young people to start discussing online friendships by asking them what is different between making friends in person and online?

Explain that this room is now an online game or chatroom, where they don't know anyone else and are looking to make a new friend.

Give each young person an identity card (Handout 12) and friendship log (Handout 12). Explain they will play this character during the activity and that this is the only information they are allowed to give in the chatroom.

Explain that when you say go, they have 60 seconds to 'meet' the person opposite, find out about them and decide whether they want to be their friend or not.

While chatting to their new potential friend, they should complete the friendship log (Handout 12) for the screen-name for that character. They should place a tick or a cross on the log to show if they want to be friends with that character.

When the 60 seconds is up, tell all YP in one of the rows to move up one seat up to the left (or if delivering virtually, swap breakout rooms) and repeat the exercise. You should continue repeating the activity until young people get back to the person they started with.

Bring young people back together and ask them to consider their friending decisions.

Ask the young people playing the following characters to stand up. BadKarma, SpinXO, Ima.robot, UFO\_Believer and Anonymouse.

Give each of these young people their hidden information card (Handout 12) and ask them to read it out. After the hidden information is revealed about each character, ask the group if it changes their decision about friending them. In response to any questions about why Shim432 might be lying about their age, take the following line: we do not know why, but what does the fact they are lying tell us about them?

Ask young people to consider their own online friends. Ask them to put their hands up if they are friends with people they know in real life. Ask them to keep their hands up if they are have any online friends who they have never met in the real world. Ask them to keep their hands up if they can be 100% sure they know every single person they are friends with is who they say they are.

Explain to young people that online it is easier for people to be someone they are not and that this can be known as catfishing. Catfishing is where someone uses a fake online persona to lure someone into a relationship. This can be a friendship or a romantic relationship, but the person they claim to be is fake.

Ask young people what they would do if they are concerned about someone they have met online or suspect them of catfishing. Signpost to CEOP, NSPCC, Childline and the Police.

## FOR DISCUSSION



Use the following questions for to help prompt discussions

- What factors affected their decision to friend someone or not?
- Refer back to the 'Qualities' list from earlier in the session. Were any of these factors?
- Was there any other information which they felt they needed before deciding?



## Captcha (Cyber Security Centre) (20 Mins)

Start by asking young people to discuss the following questions in pairs or small groups.



### FOR DISCUSSION

- What is CAPTCHA?
- What does CAPTCHA stand for?
- Where have you seen CAPTCHA's?

Bring young people back together and using the definition on Page 32, explain that CAPTCHA's are programs that challenges a users response to determine if they are a human or a computer. Explain that they are used to protect against harmful activity that can be caused by automated programs accessing a site. Suggest that young people will probably have seen these when trying to access online banking, websites, social media and more.

Ask young people to return back to their groups and discuss the following:



### FOR DISCUSSION


- What are the benefits of CAPTCHA?
- Are there any disadvantages to CAPTCHA? If so, what are they?

Bring young people back together to discuss their thoughts. Explain that although CAPTCHA's are beneficial and make websites more secure, they aren't easily accessible for everyone and it can be frustrating as it takes longer for you to get onto websites.

Give young people a piece of flipchart paper and a pen and ask them to spend 10

minutes coming up with their own CAPTCHA . Allow access to the internet to help young people brainstorm ideas. Suggest it could be letters or words or it could even be a puzzle, jigsaw or spot the difference.

Once young people are finished, ask them to swap with one another and try to complete the CAPTCHA's one another have come up with.

Please cut here  .....

## HANDOUT 10

### TRUE OR FALSE

- **Everything you read online is accurate / true. FALSE** - Not everything we read online is true and cannot be trusted to be accurate all the time.
- **Online Quizzes / Games on social media overwrite your privacy settings. TRUE** - When you complete a quiz on facebook, or play a game on snapchat / messenger, the settings for the game, overwrite your settings. This means that some of the information you put into the game / quiz can be made public or shared without your consent.
- **Fake news is only created by people who want to get famous. FALSE** - Lots of people spread fake news, for a whole host of reasons, not simply just to get famous, although this can be a motivating factor for some.



# HANDOUT 10 TRUE OR FALSE

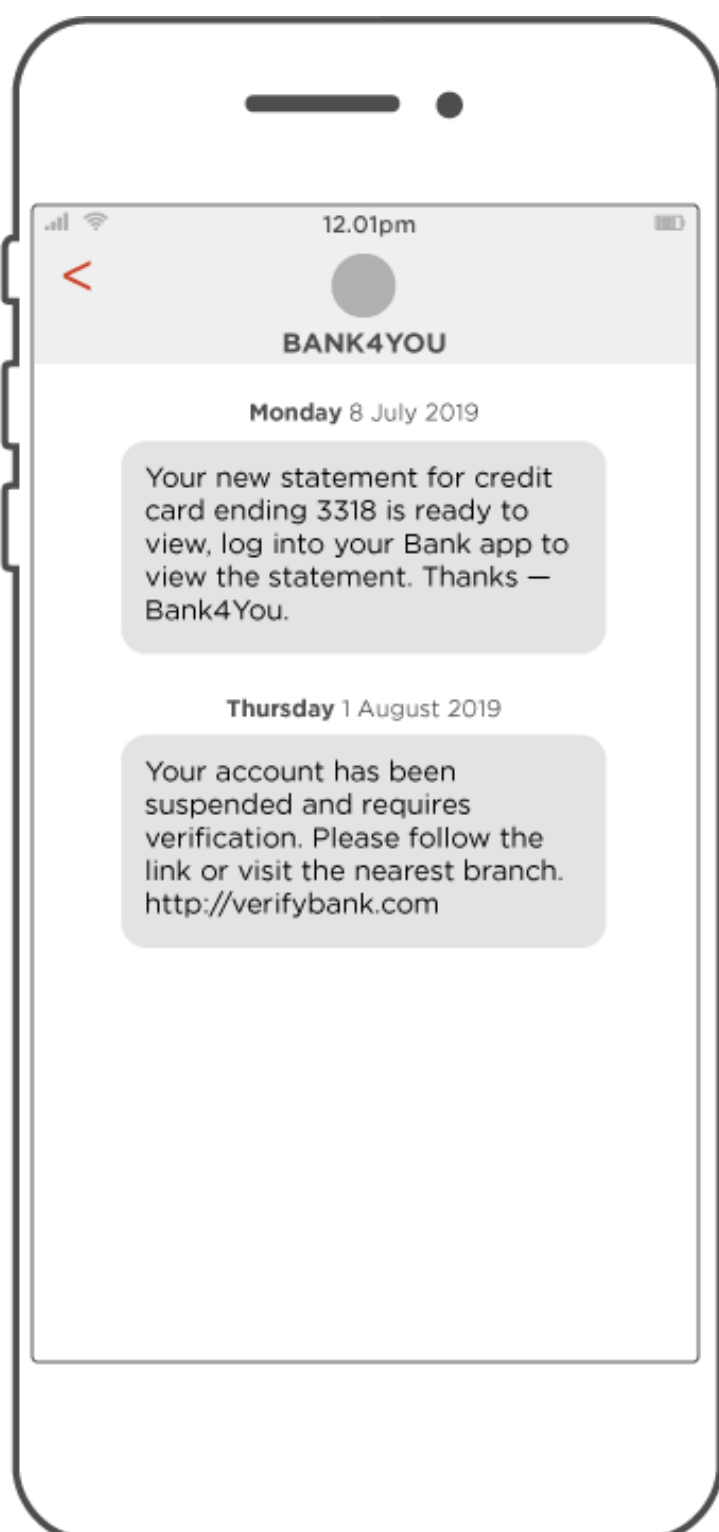
- **All news outlets can be trusted to tell the truth. FALSE** - Most news outlets tell the truth and report news accurately. However, they sometimes overexaggerate, miss out pieces of information and leave out important details. This means that they cannot be trusted to tell the truth 100% of the time.
- **You can tell by the hyperlink whether or not something is likely to be fake news. TRUE** - You can normally tell by the hyperlink if the website is legitimate or not. 9 times out of 10 if a hyperlink has lots of characters and is very long, it is likely to be illegitimate and therefore the information on the website cannot be trusted 100%.
- **Fake news is always 100% untrue. FALSE** - Some aspects of fake news articles are based on truth, but may be exaggerated or a false impression of facts given.
- **It is thought that around 25% of people have visited a fake news website and used this for information to share with others. TRUE** - A quarter of people at least are estimated to visit fake news sites on a weekly basis. This may be because they are looking for information and unknowingly found something false, or they may be looking for fake news.

Please cut here

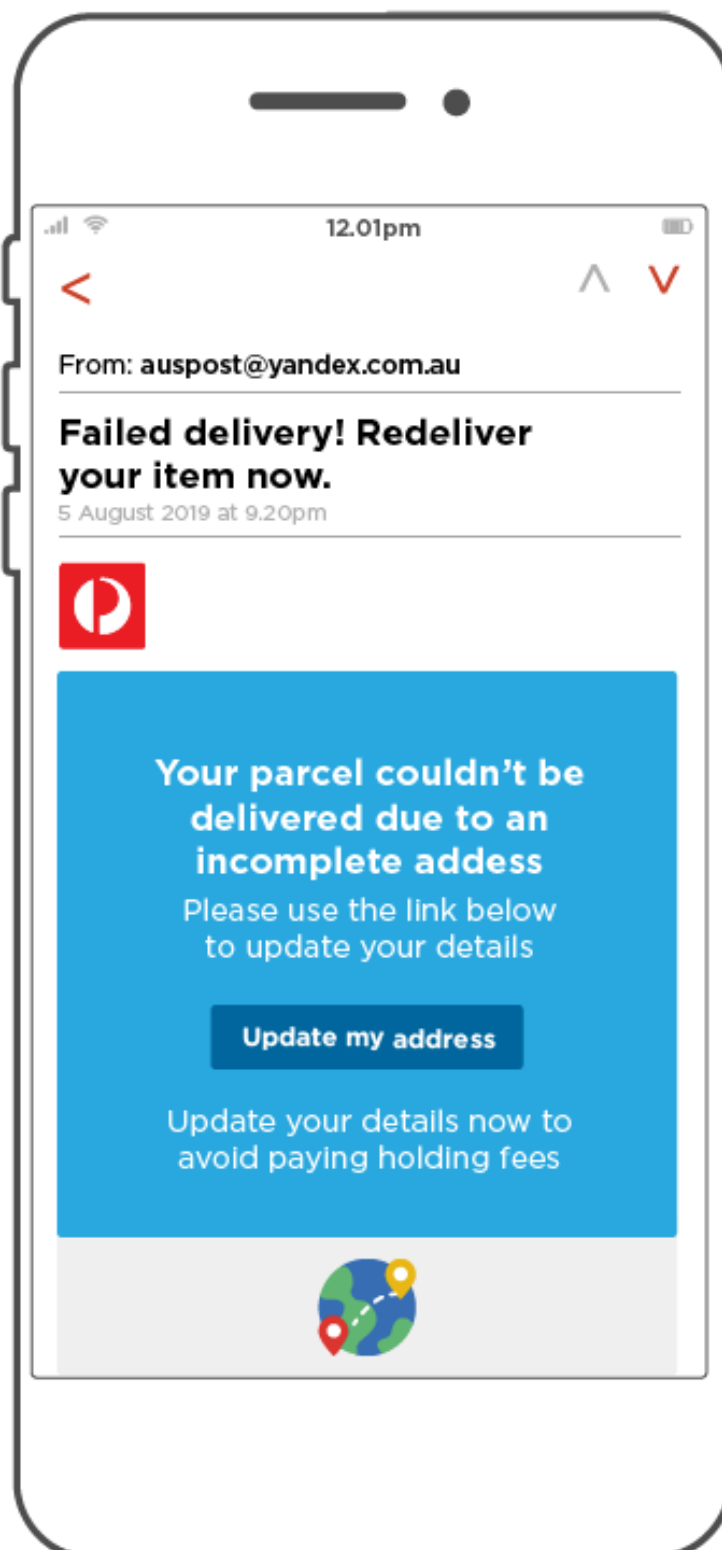


# HANDOUT 11 SPOT THE SCAM

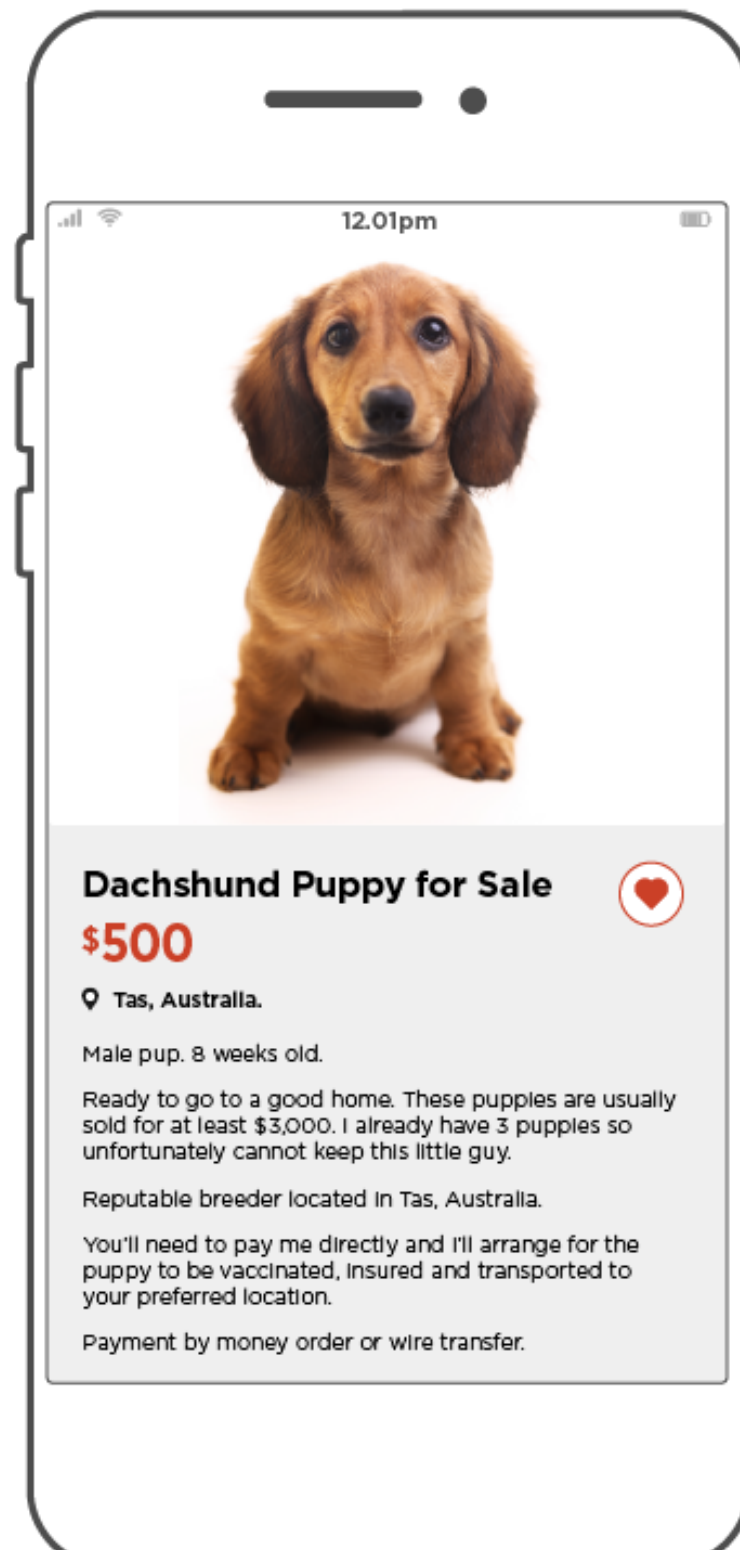
1.



2.



3.




# HANDOUT 11 SPOT THE SCAM


4.

World of BBQ

http://bigworldofbbqz.com/familybbq

**BIG WORLD OF BBQS** LOG IN | MY ORDER | MY ACCOUNT |  \$AUD ▼

Home Products Customer Info Search ...




**Limited time only**  
0D 6H 1M 32SEC

**Family BBQ**  
~~\$767~~ \$267

\*pay by bank transfer for a further 10% off

**ADD TO CART**

5.



Friday 02/02/19 4.18pm  
Doe, John <john@services.com.au>  
**URGENT: supplier will not complete an urgent order**

To Sandra@services.com.au

---

Hi Sandra

Sorry to spring this on you with late notice - I need you to make an urgent payment to AusTekno Logics' new bank account ASAP or they won't deliver on time.

I'll be in a meeting all day.

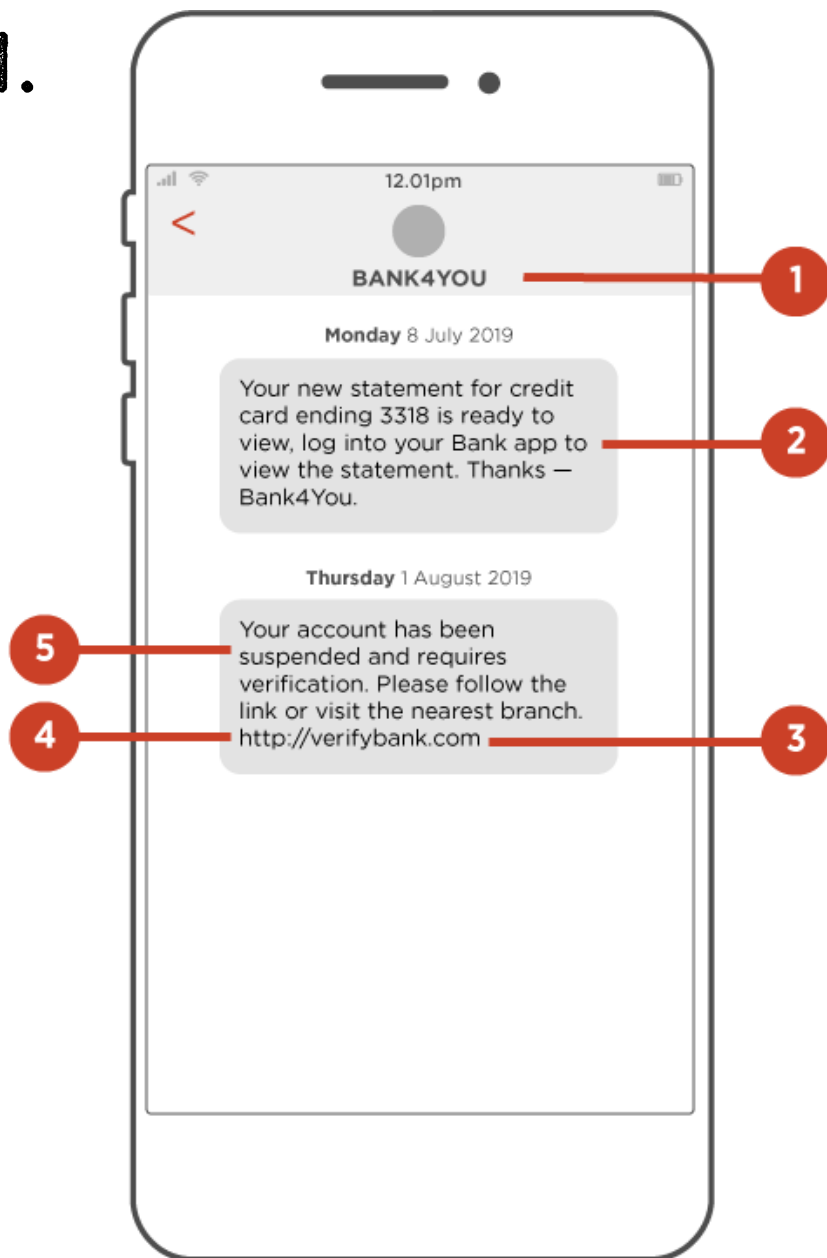
AusTekno Logics  
Account number: 123456789  
Code: 11 22 33

Thanks,

John Doe  
The Services Company  
Chief Executive Officer  
Email: john.doe@services.com.au

# HANDOUT 11 SPOT THE SCAM ANSWERS

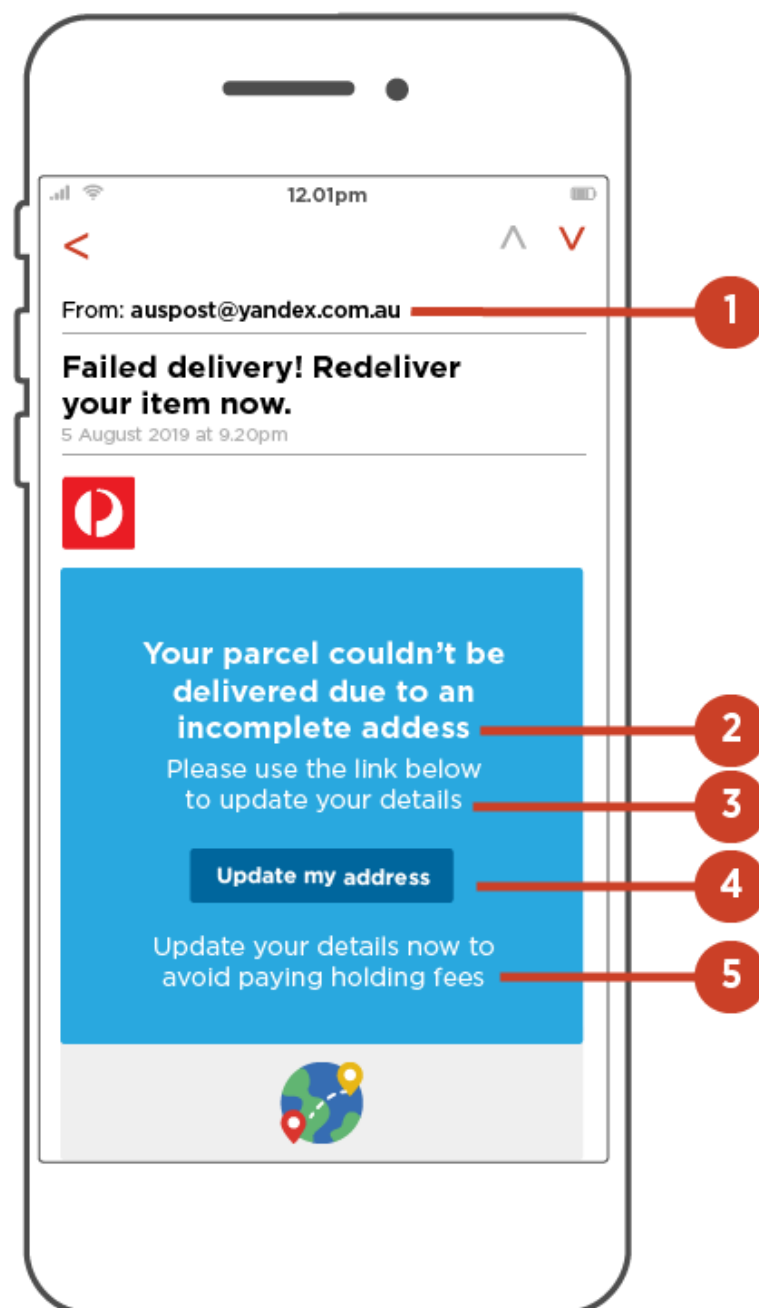
1.



## PHISHING SCAM: BANK SMS

1. **Scammers can make messages look real.** Even if you've previously received legitimate SMS messages from the same number, don't assume all following messages are real.
2. **It's different in style from the first SMS.** The previous SMS is legitimate and it provides information only. It tells you to log into your account but provides no links that could lead to potentially malicious websites.
3. **It has a malicious link.** The new SMS contains a link to a phishing website. These types of websites attempt to trick you into giving out personal information such as your bank account details, passwords and credit card numbers.
4. **It's not secure.** Legitimate sites containing sensitive information will use https not http, but don't rely on this alone – some scam sites use https too.
5. **It has a sense of urgency.** Scams often try to create a sense of urgency. Don't rush – take the time to think about what the message is telling you to do and consider whether it's real.

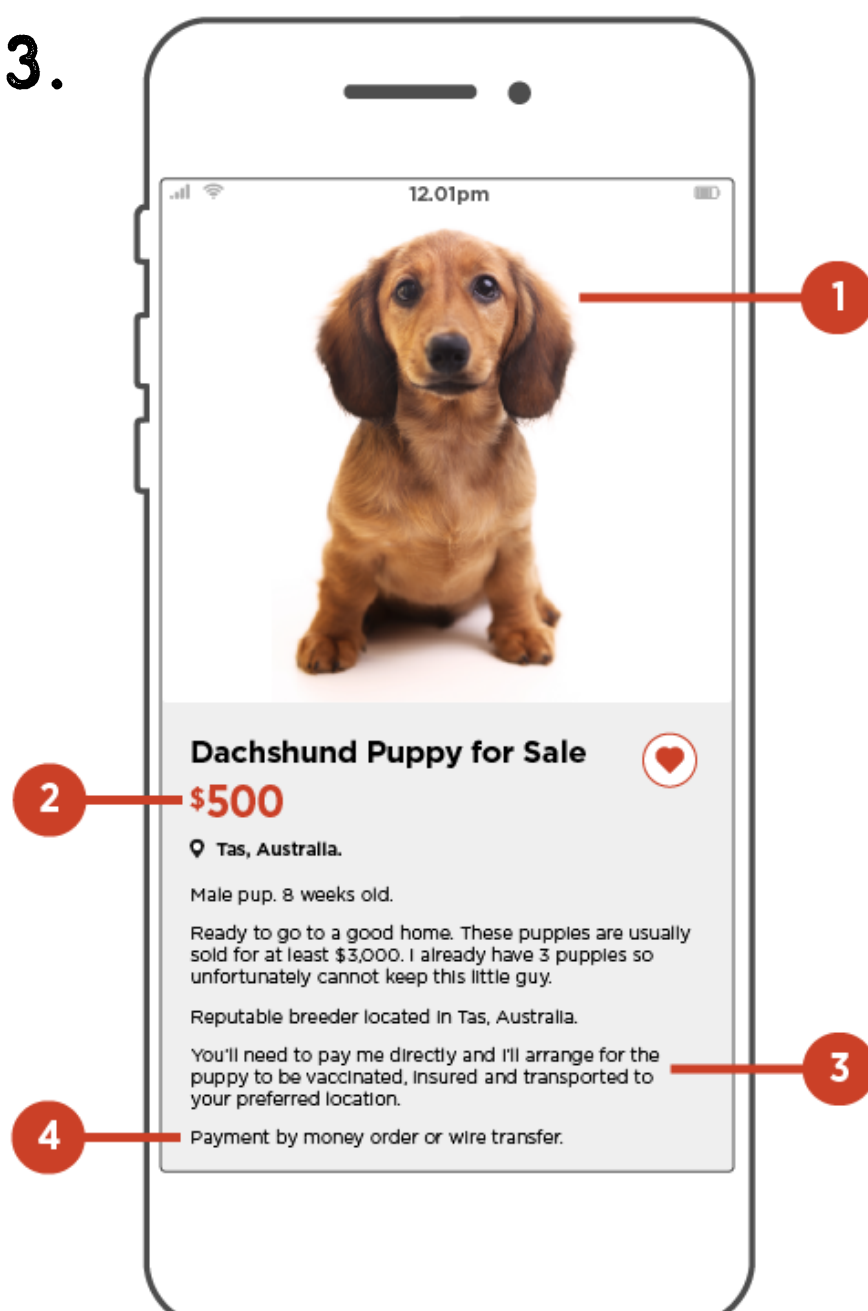
2.



## PHISHING SCAM: MAIL DELIVERY

1. **You can't confirm who it's from.** Check that the email address of the sender is authentic. In this example, the domain name (the part of the email address after the @ symbol) is a sign that it's not real. If you're unsure, contact the business directly using contact details that you've sourced independently and you know are legitimate.
2. **It has spelling and grammatical errors.** These types of errors are a sign that it could be a scam.
3. **It has a request for you to do something.** The email is trying to obtain your personal details. If scammers gain access to your personal information they can potentially steal your identity or target you with a scam. Be cautious when providing your details.
4. **It has a malicious link.** Don't just be wary of attachments. Watch out for links to phishing websites.
5. **There's a sense of urgency.** Scammers try to create a sense of urgency to encourage you to do something quickly. Don't rush – take the time to consider and check whether an email is real.

3.



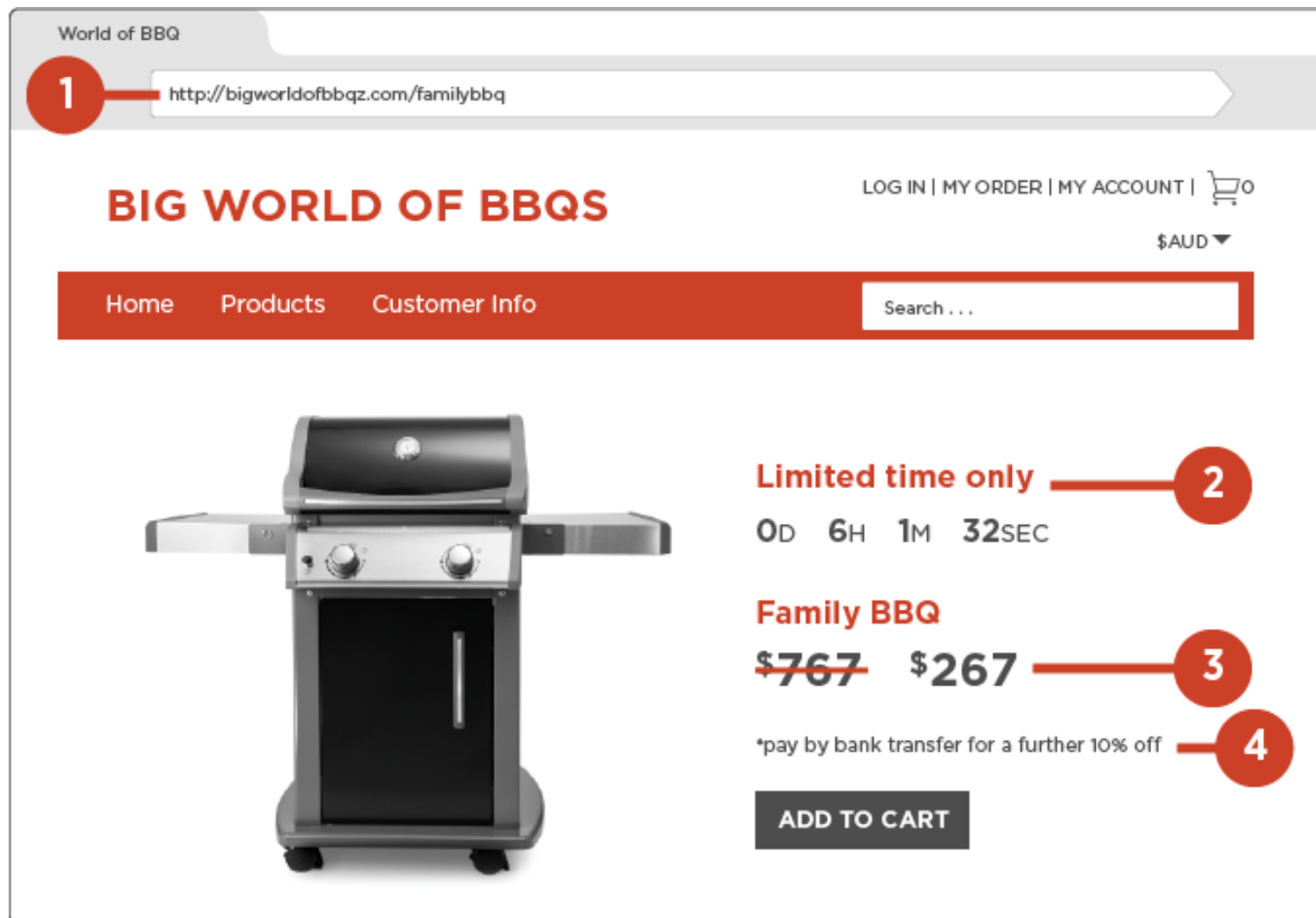
## CLASSIFIED SCAM

1. **There's no evidence of the puppy.** Puppy scammers often steal photos from legitimate breeders' websites and post them on their own. Use image search services such as Google or TinEye to do a reverse-image search to find out if a picture has been posted elsewhere on the internet. Never trust photos alone – always ask to see the puppy in person and, if that's not possible, ask for additional photos and videos.
2. **It's too good to be true.** The price might be enticing, but remember that scams often present offers that really are too good to be true.
3. **There are other up-front costs to consider.** Puppy scammers often claim that they live or have moved interstate or overseas, so you'll need to pay extra costs like transport, insurance or customs costs. Local pickup will usually not appear as an option.
4. **The payment method is not secure.** Think about how they're asking you to pay. Scammers often ask you to pay by non-secure payment methods. It's rare to recover money sent this way. Always look for secure payment options such as PayPal or credit card.



# HANDOUT 11 SPOT THE SCAM ANSWERS

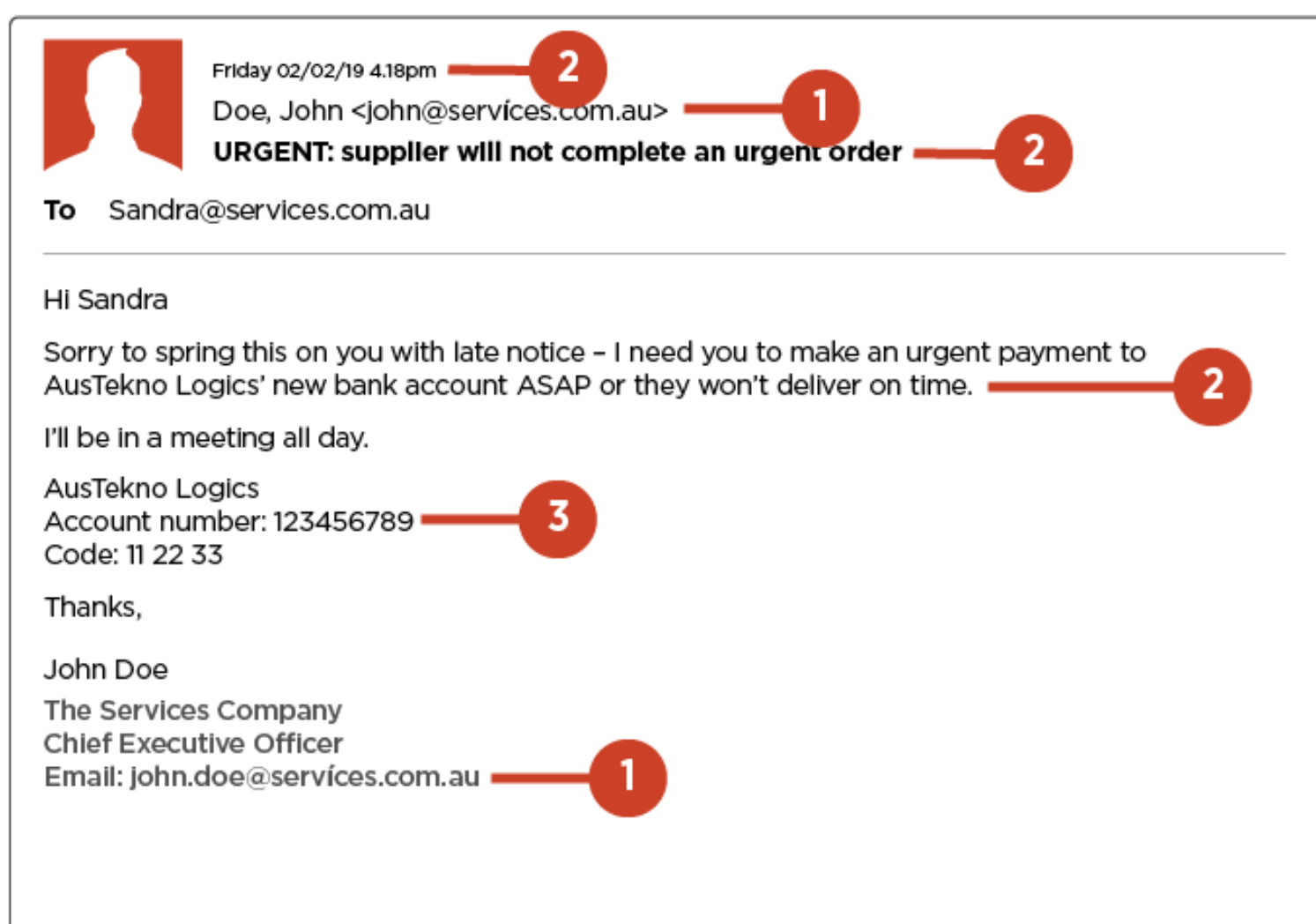
4.



## ONLINE SHOPPING SCAM

1. **It's not secure.** When online shopping, always look for the https (not http) and the padlock icon in the address bar to ensure there's a secure connection between you and the website.
2. **It has a sense of urgency.** Scammers try to create a sense of urgency to encourage you to do something quickly. Don't rush – take the time to do your research and consider whether a website is real.
3. **The deal is too good to be true.** The price might be enticing, but remember that scams often present offers that really are too good to be true.
4. **It's using a non-secure payment method.**

5.



## BUSINESS EMAIL COMPROMISE SCAM

1. **You can't confirm who it's from.** Scammers often use email addresses that are similar to a real email address. Check that the sender's email address is the real one. Look carefully – the letter 'i' in 'services' is actually a different character.
2. **It has a sense of urgency.** Don't rush – take the time to consider and check whether an email is real.
3. **Some things have changed.** Business email compromise scammers will try to divert payments to their own bank accounts. Always verify changes to payment details directly with the recipient, using known and trusted contact details.

# HANDOUT 11 SPOT THE SCAM TIPS

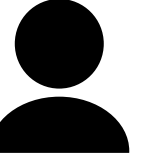
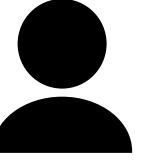
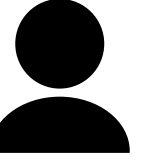
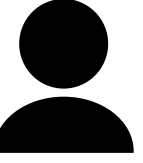
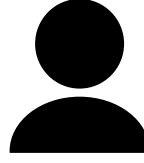
It's easier to spot a scam if you know what to look for. Remember to be careful if someone:

- You don't know contacts you out of the blue.
- You've never met in person asks for money.
- Asks you to pay for something or to give them money through unusual payment methods such as gift cards, wire transfers or cryptocurrencies.
- Asks you to pay for something in advance – especially through an unusual payment method.
- Asks you for personal information, like your bank details or passwords, or access to your computer.
- Pressures you into buying something or making a decision quickly.
- Offers you something that sounds too good to be true – like an online shopping deal, a prize for winning a competition, an unclaimed inheritance or an invitation to invest in an 'amazing' scheme.

# HANDOUT 12 SPEED FRIENDING CARDS

 <p><b>Screen Name</b> Footiemad16 <b>Age</b> 16 <b>Hobby</b> Football <b>Interesting Fact</b> Speaks 5 Languages</p>	 <p><b>Screen Name</b> BadKarma <b>Age</b> 14 <b>Hobby</b> BMX <b>Interesting Fact</b> Broken Both Leggs</p>	 <p><b>Screen Name</b> google_was_my_idea <b>Age</b> 16 <b>Hobby</b> Gymnastics <b>Interesting Fact</b> Miss Teen GB</p>	 <p><b>Screen Name</b> OP_rah <b>Age</b> 13 <b>Hobby</b> Blogging <b>Interesting Fact</b> 10,000 Twitter Followers</p>	 <p><b>Screen Name</b> username_copied <b>Age</b> 11 <b>Hobby</b> Volunteering <b>Interesting Fact</b> Pet snake &amp; tarantula</p>
 <p><b>Screen Name</b> SpinXO <b>Age</b> 15 <b>Hobby</b> Taking Photos <b>Interesting Fact</b> Took GCSEs aged 7</p>	 <p><b>Screen Name</b> Lil2003 <b>Age</b> 13 <b>Hobby</b> Designing Comics <b>Interesting Fact</b> Has visited countries on every continent</p>	 <p><b>Screen Name</b> Anonymouse <b>Age</b> 12 <b>Hobby</b> Fashion <b>Interesting Fact</b> Is a Vegan</p>	 <p><b>Screen Name</b> ashley_said_what <b>Age</b> 12 <b>Hobby</b> Inventing apps <b>Interesting Fact</b> First in App of the Year competition last year</p>	 <p><b>Screen Name</b> Abi04 <b>Age</b> 16 <b>Hobby</b> Social Networking <b>Interesting Fact</b> Parents were 80s rock stars</p>
 <p><b>Screen Name</b> Ima.robot <b>Age</b> 15 <b>Hobby</b> Collecting things <b>Interesting Fact</b> Parents are millionaires</p>	 <p><b>Screen Name</b> UFO_Believer <b>Age</b> 14 <b>Hobby</b> Extreme Sports <b>Interesting Fact</b> Has a criminal record</p>	 <p><b>Screen Name</b> LolaD12 <b>Age</b> 13 <b>Hobby</b> Movies / Theatre <b>Interesting Fact</b> Loves Thai Food</p>	 <p><b>Screen Name</b> PartySam15 <b>Age</b> 15 <b>Hobby</b> Camping <b>Interesting Fact</b> Doesn't own a mobile phone</p>	 <p><b>Screen Name</b> ihazaquestion <b>Age</b> 18 <b>Hobby</b> Driving my car <b>Interesting Fact</b> Sang on reality TV</p>

# HANDOUT 12 HIDDEN INFORMATION

 <p><b>Screen Name</b> BadKarma <b>Hidden Truth</b> Claimed to be 14, but in reality is actually 32.</p>	 <p><b>Screen Name</b> Ima.robot <b>Hidden Truth</b> Collects naked selfies in their spare time.</p>	 <p><b>Screen Name</b> SpinXO <b>Hidden Truth</b> Takes pictures of people getting dressed in changing rooms and posts them anonymously online.</p>	 <p><b>Screen Name</b> UFO_Beileiver <b>Hidden Truth</b> Criminal record is for shoplifting sweets from a supermarket when they were 11. They have not committed any crime since.</p>	 <p><b>Screen Name</b> anonymouse <b>Hidden Truth</b> Has a blog where they post messages and photos of people they dont like online and bullies them.</p>
---	---	--	--	---

# HANDOUT 12 FRIENDSHIP LOG

NAME: \_\_\_\_\_

USERNAME:	AGE:	HOBBY:	INTERESTING FACT:	FRIEND:
Footiemad16				
BadKarma				
google_was_my_idea				
OP_rah				
username_copied				
SpinXO				
Lil2003				
Anonymouse				
ashley_said_what				
Abi04				
Ima.robot				
UFO_Believer				
LolaD12				
Partysam15				
Ihazaquestion				

NOTES, THOUGHTS, QUESTIONS, IDEAS!



**DIGITAL SAFETY** —

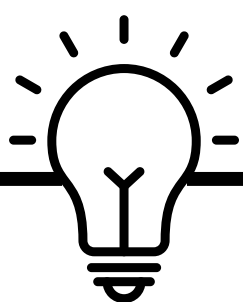
# SESSION 4

## INTRODUCTION

Session 4 is all about Digital Safety. It explores 2 Factor Authentication, Virus', Passwords & Privacy.

## SESSION OVERVIEW

- Code Breaker **(20 Minutes)**
- Privacy Settings Quiz **(15 Mins)**
- Secure Password Challenge **(5 Mins)**
- Escape Room - Virus', Password Protection & Anti-Virus Software **(1 Hour 20 Mins)**



### TOP TIP

for young people to get the most out of the Escape Room, they will need a device between 2 or 3 at the most. iPad's and Laptops are best.

## RESOURCES

- ➔ Handout 13 - Code Breaker.
- ➔ Handout 14 - Privacy Settings Quiz.
- ➔ Several Devices with an Internet Connection.

## LEARNING OUTCOMES

Young People will:

- ✔ Develop Cyber Resilience Skills.  
Use a password manager to generate strong passwords.
- ✔ Understand two factor authentication.  
Learn to keep devices secure.

- ✔ Build their knowledge of cyber resilience and understand how to put this into practice.

## DELIVERY NOTES

Prior to delivering the session, Youth Workers should:

- Read through the session plan, key terms and familiarize themselves with the resources.
- Check the internet connection is working and load the escape room.

## OPENING ACTIVITIES

### Code Breaker (20 Mins)

Split young people into 3 teams. Give each team a different code and cipher. Task each group to decode the message they have been given using their cipher.

Once young people have decoded their messages, give each group a blank cipher and ask them to come up with their own code and coded message. Then, ask the groups to swap these over and decode one another's messages.

Explain to young people that the focus of today's session is exploring virus' and 2 factor authentication. Encourage young people that the problem solving and critical thinking skills they have just applied, they will need to continue to use throughout the session, especially when working to solve the escape room.

## DEVELOPMENT

### **Privacy Settings Quiz (15 Mins)**

Give each young person a copy of Handout 14 (Privacy Settings Quiz). Ask them to complete this on their own.

Once young people have completed the quiz, bring them back together and go through the answers. If there is anything that surprises or shocks young people, spend time discussing this and exploring their thoughts further.

Explain to young people that it might be helpful to remember some of this information as they might need it later on.

### **Secure Password Challenge (5 Mins)**

Explain to young people that part of their Escape Room challenge will involve learning about secure passwords.

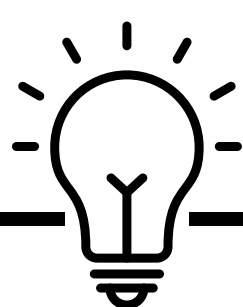
Ask young people to come up with what they think a strong password would look like.

Take it in turns for young people to enter these into the following 2 websites to check if they are secure.

Explain that one of the websites will give them some passive aggressive advice on their password strength, and the other will give them practical tips on how to make their password more secure.

**Passive                  Aggressive                  Passwords**  
**(trypap.com)**

**How Secure Is My Password? | Password Strength Checker (security.org)**



### **TOP TIP**

Make sure young people know not to use one of their own passwords.

### **Escape Room (1 Hour 20 Mins)**

For the rest of the session, young people will be asked to work in groups of no more than 3 to solve the Cyber Resilience Escape Room.

The Escape Room is themed around a virus which has corrupted someone's phone and young people's task is to work through a series of cyber related challenges to defeat the virus and save the data it is threatening to steal. Young people will need to use all the skills and knowledge they have learned so far to complete this challenge and it should take them roughly 1 hour to do.

All challenges are contained within the escape room, although it might be helpful for them to have paper and pens to be able to work out some of the codes and take notes.

To access the escape room, visit the Digital Youth Work Padlet (linked below) where you will find the most up to date version of this. As it is constantly being updated by young people, this is the best way to ensure playing it is a smooth experience.  
**[https://padlet.com/youth\\_work\\_dg/digitalyouthwork](https://padlet.com/youth_work_dg/digitalyouthwork)**

After completion of the escape room, encourage young people to work as group to discuss how they found it. What surprised them? Was there anything that they didn't expect? If so, what? Do they think situations like what was described in the Escape Room happen in real life? Where would they go for support if they found themselves in a situation like this?





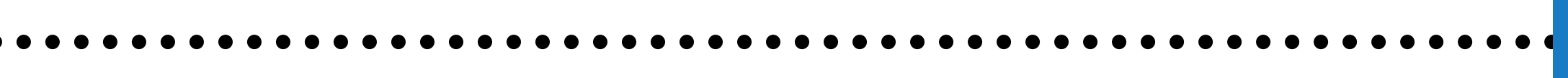
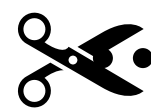


# HANDOUT 14 PRIVACY SETTINGS QUIZ

## Quiz Sheet:

- 1. How can should you make your social media accounts private and secure?**
  - a. Always tagging friends.
  - b. Using security applications.
  - c. Making a strong password.
  - d. Going offline intermittently.
- 2. Which of these is not a privacy feature on Instagram?**
  - a. Block comments.
  - b. Remove a follower.
  - c. Protect my Tweets.
  - d. Stop Direct Messages.
- 3. Which of these privacy settings is not specific to Twitter?**
  - a. Disable direct message.
  - b. Remove follower.
  - c. Protect my tweets.
  - d. Password Protect.
- 4. Which of these settings is unique to WhatsApp?**
  - a. Last Seen.
  - b. Password Protect.
  - c. Remove Follower.
  - d. Protect my Tweets.
- 5. Which of these is usually not kept private on social media?**
  - a. Photos.
  - b. Username.
  - c. Followers.
  - d. Likes.
- 6. Which of these social media platforms features end to end encryption?**
  - a. Facebook.
  - b. Snapchat.
  - c. Twitter.
  - d. WhatsApp.

Please cut here



## Quiz Answers:

1. Making a Strong Password.
2. Public Profile.
3. Password Protection.
4. Last Seen.
5. Username.
6. WhatsApp



**CREATORS 4 CHANGE**



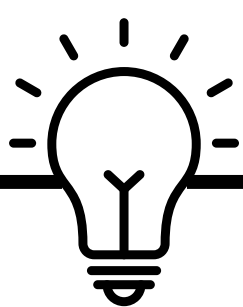
# SESSION 5

## INTRODUCTION

Session 5 is the final session of the Cyber Resilience Toolkit. It aims to consolidate what young people have learned and help them to develop digital skills for the future.

## SESSION OVERVIEW

- Braindump (30 Mins)
- Our Digital Footprint (30 Mins)
- Let's Make an Inspiring Internet - Be Internet Citizens (45 Mins)
- Creators for Change (15 Mins)



## TOP TIP

The whole session should last for 2 hours. If you are short on time, focus on Our Digital Footprint and Let's Make an Inspiring Internet.

## RESOURCES

- ➔ Flipchart Paper.
- ➔ Handout 15 - Our Digital Footprint.
- ➔ Marker Pens.
- ➔ Mobile Phones or Tablets.
- ➔ Access to the Internet.

## LEARNING OUTCOMES

Young People will:

- ✔ Explore and understand the long term impact of a digital footprint.
- ✔ Begin to connect knowledge and skills about cyber resilience with opportunities for careers.
- ✔ Understand ways in which the internet can be used positively.

- ✔ Recognize the importance of Digital Citizenship.

## DELIVERY NOTES

Prior to delivering the session, Youth Workers should:

- Read through the session plan, key terms and familiarize themselves with the resources.
- Ensure all devices are connected to the internet and fully charged.

## OPENING ACTIVITIES

### Braindump (30 Mins)

Start the session by explaining to young people that this is the final session of the programme and so is designed to help them reflect on everything they have learned.

Split young people into 4 groups and give each group a piece of flipchart paper and a marker pen. Ask each group to write down one of the following headings:

1. Digital Rights
2. Social Media
3. Cyber Crime
4. Digital Safety

Give each group 5 minutes to 'braindump' everything they can remember about the session on their piece of flipchart. Encourage young people to think about any stand out moments or things that surprised / shocked them.

After 5 minutes, swap the flipchart around and ask young people to repeat this adding to what other groups have written down. Repeat until all groups have had each piece of paper.

Then, ask for a volunteer from each group to read out what has been written underneath each of the headings.

Conclude that in a short space of time, the group have learnt a lot about cyber resilience and today is about putting some of that into practice.

## DEVELOPMENT

### Our Digital Footprint (30 Mins)

Start by asking young people what they think a digital footprint is.

### KEY TERMS

**Digital Footprint** – A digital footprint is the trail of information you leave behind when you use the internet.

Use the definition above to explain to young people what a digital footprint is. Explain that a digital footprint isn't necessarily good or bad. It exists and your thoughts and feelings about it and the effects it has on you depend on a lot of different factors such as your values, priorities, age, life stage, school and family expectations.

Explain that your digital footprint is made by things that are visible such as social media posts from you and other people. This includes photos, status updates, check-ins at locations, online groups and sites that you've liked or joined, and posts from other people that you've shared.

It also includes things that can be learned about you based on your activity such as websites you visit, personal information you enter, messages and emails you send, and so on.

Ask young people for suggestions of famous people to search for online. As a group search for those people to give an idea of how easy it can be to find content about individuals.

Then, ask young people to work in small groups and make lists of words that describe the type of content they find when they search for those famous people. Make different lists for each person. Share some of those words with the larger group.

Bring young people back together and discuss using the following questions to help prompt discussions.

### FOR DISCUSSION

- Are these words mostly positive? Negative?
- How do you think these people feel about their online presence?
- How would you feel if all of this information was out there about you?

Hand out the My Digital Footprint worksheet (Handout 15). Ask young people to work individually or in pairs to explore their own online presence.

Ask them look at all the social media sites they use (Snapchat, Instagram, Facebook, LinkedIn, Twitter, etc.) and also do an internet search of their names. What do they find? What do they think about that? Are there things they would like to change? Has anyone tagged you in something that makes you uncomfortable or gotten access to your accounts and posted about you?

Bring young people back together and



talk about what they found. Were there any surprises? Do they have any ideas for things they'd like to change?

If young people do want to change their digital footprint suggest they could do some of the following:

Tighten restrictions on social media. Only accept friend/follow requests from people you know in real life. Set privacy setting so that information about you (including images) is not visible to the public. Change settings, if necessary, so that others need your permission to tag you in posts.

Delete things that you don't want others to see. They may not completely go away if they have been shared by others or stored somewhere, but you can usually at least make them harder to find. Reset passwords. Make sure they are strong and do not share them! Carefully consider every time you post or share whether you want it to live on forever, because it might.

Conclude with young people the importance of their digital footprint, using the example that some people have lots jobs based on this and something they said when young that has stayed in their footprint forever.

### **Let's Make an Inspiring Internet (45 Mins)**

Split young people into small groups and explain that they have 30 minutes to come up with a short 3 minute presentation raising awareness of digital citizenship.

Explain this will require them to use their learning from all the sessions, so they might want to use their 'braindump' flipchart to help them think about what they want to talk about.

Explain to young people that their campaign can take on any form, but they might want to think about some of the following as ideas to get them started:

- a. A performed presentation
- b. A digital presentation
- c. A role play scene
- d. A spoken word piece
- e. A song
- f. A poster for the organisation

Encourage YP to map out their awareness campaign on flipchart paper, and to include some of the following:

- An overview of what they have learnt.
- Key takeaway facts from each session.
- How you can stay safe online.
- How you can make the internet a better, and safer place to be.
- What they hope the internet will be like in the future.

Once young people have made their presentations allow 15 minutes for each group to present what they have come up with. If young people have written consent, and they give permission, you could also film these for social media.

## REFLECTION

### **Creators for Change (15 Mins)**

Spend the last 15 minutes of the session supporting each young person to make a pledge of how they will put what they have learned into action. Again refer back to the flipchart braindump if needed.

Finish the session by handing out young people's cyber resilience badge, and encouraging them to be champions of change in their communities.

CREATORS  
OF  
CHANGE  
CYBER RESILIENT CITIZENS



ADD US @YOUTHWORKDG

