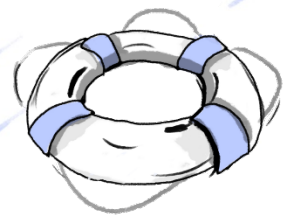


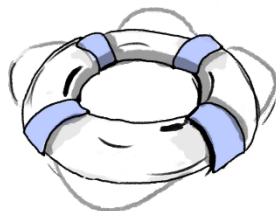
MY CYBERABILITY PLAN



Name: _____



CYBERABILITY



CYBERABILITY

This workbook is a companion to free online cybersafety training available at

www.cyberability.org.au

Authors: The CYBERABILITY team: Dr Kate Gould, Colin Brokenshire, Anna Holliday, Alf Archer, Jao Carminati, Malachi Cloak de Paul and Professor Jennie Ponsford

Design: A.D Lester Illustration; Inclusive Creatives, Format FixIT

Published: 2021, Melbourne, Australia

Project Partners



MONASH
University



Li-Ve
TASMANIA

Funded By



**TRANSPORT
ACCIDENT
COMMISSION**

Navigating **Online** Risks

This CYBER**ABILITY** training is designed with and for people with brain injury to help you navigate online risks.

Everyone will plot their own course online and need their own Cyber **Safety** Plan.

Complete these activities after finishing each topic to help switch on your cyber safety skills.

**Stay
Scam
Safe**



Navigating Your Plan

Topic	Page
The Nautical Theme	5
1 What is a Scam?	6
2 Scams and Brain Injury	8
3 What are Red Flags?	10
4 Romance Scams	12
5 Gaining Access Scams	14
6 Increasing Your CYBERABILITY	16
7 Stopping a Scam	20
8 Finding the Silver Lining	24
Extra Support	26



The Nautical Theme

Why do we use the captain at sea metaphor?

The internet is a bit like the ocean.

Whenever you go online or use your phone, it's like you're the Captain setting off on a voyage.

At sea and online are lots of fun and interesting things.

But, just like in the ocean, there are dangers when you go online.

On the cyber seas, one of the risks is being taken for a ride into dangerous waters, where you could get scammed.



What is a **SCAM**?

Scams are crimes where someone tries to rip you off



What is a Scam?

How would you describe what a scam is, in your own words?

Scams can happen on any online platforms and using any technology.

A platform is any sort of device, application or website that you might use to talk to people, browse online or play games.

This is a list of different technologies and platforms that many people use.
 Tick the ones that you use.

I use these platforms:

- | | |
|--|---|
| <input type="checkbox"/> Email | <input type="checkbox"/> Online games |
| <input type="checkbox"/> Mobile phone call | <input type="checkbox"/> <i>Words with Friends</i> |
| <input type="checkbox"/> Text messaging | <input type="checkbox"/> <i>Other:</i> |
| <input type="checkbox"/> Tablet/iPad | <input type="checkbox"/> Online shopping |
| <input type="checkbox"/> Computer/laptop | <input type="checkbox"/> <i>Gumtree</i> |
| <input type="checkbox"/> Smartwatch | <input type="checkbox"/> <i>eBay</i> |
| <input type="checkbox"/> Fax | <input type="checkbox"/> <i>Facebook marketplace</i> |
| <input type="checkbox"/> Landline/home phone | <input type="checkbox"/> <i>Other:</i> |
| <input type="checkbox"/> Social Media | <input type="checkbox"/> Dating sites/Apps |
| <input type="checkbox"/> <i>Facebook</i> | <input type="checkbox"/> <i>eHarmony</i> |
| <input type="checkbox"/> <i>Instagram</i> | <input type="checkbox"/> <i>Other:</i> |
| <input type="checkbox"/> <i>Twitter</i> | <input type="checkbox"/> Online banking or paying bills |
| <input type="checkbox"/> <i>Other:</i> | <input type="checkbox"/> <i>Other:</i> |

Remember, anyone can be scammed on any platform.

It is important to look out for scams no matter what site or platform you are on.

If you are not sure, ask someone you trust.

Scams and **BRAIN INJURY**

Whilst most online experiences are safe and positive, cyberscams can happen to anyone.

People with an acquired brain injury may be more likely to have problems online, such as being scammed.

When people with brain injury are scammed, they have worse problems than someone without a disability.

For example, it might be harder to earn back the money sent to scammers.



Scams and Brain Injury

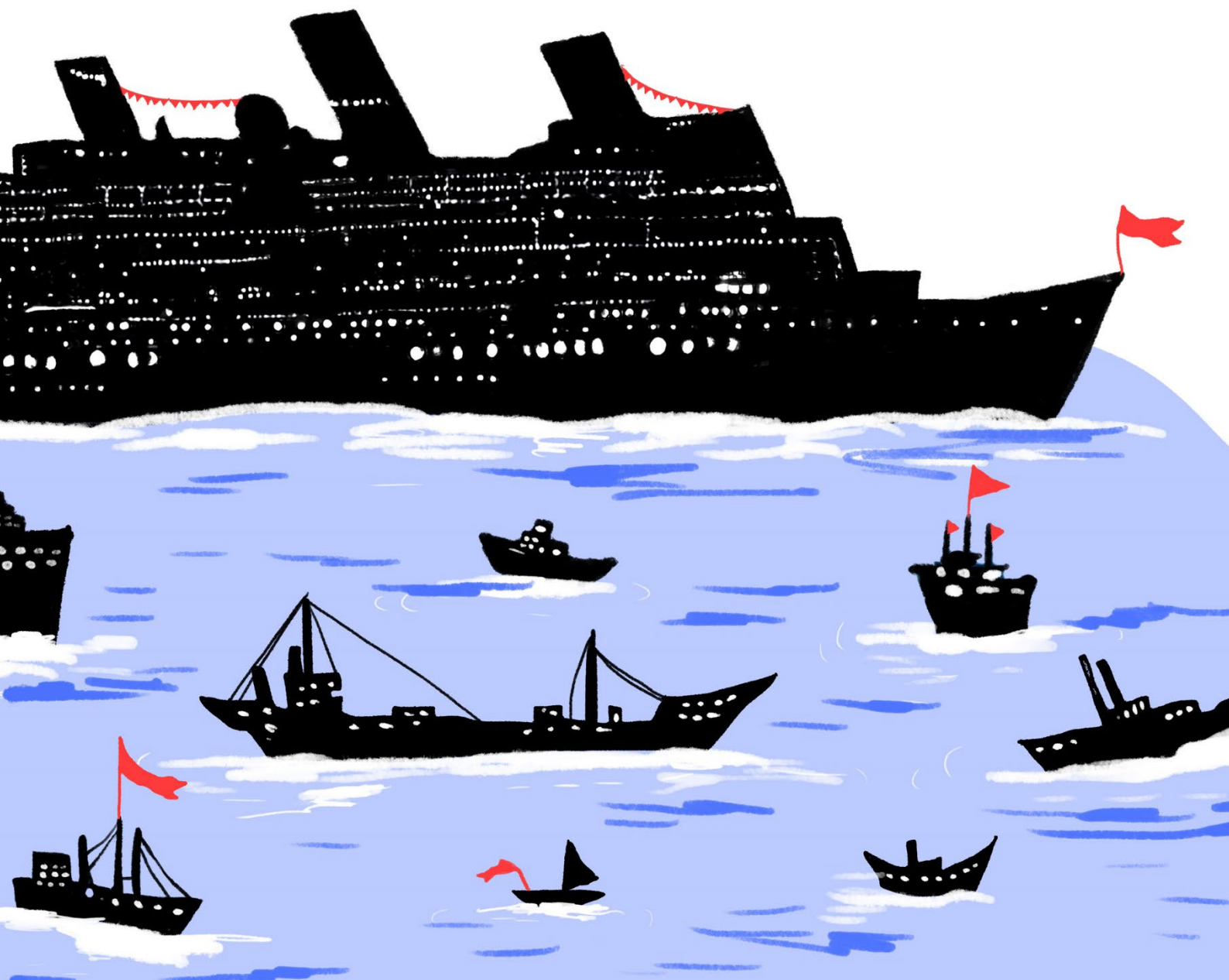
Tick which changes you have experienced from your brain injury and write down how you could apply each TIP to your life in the notes section.

You may find it helpful to [ask someone you trust](#) to help you come up with ideas for how you could do this and what actions you will take.

My Scam Risks	Tips for Increasing my CYBERABILITY	What I'll Try:
<input type="checkbox"/> Not being aware I have been scammed	Stay alert for scams when you're online.	
<input type="checkbox"/> I don't know about scams (scam blindness)	Remember, scams exist and can happen to anyone and on any website, app or mobile phone.	
<input type="checkbox"/> I'm very trusting and generous	Be very careful who you trust. It's good to have a healthy level of scepticism or doubt with strangers.	
<input type="checkbox"/> I spend a lot of time online	Reduce the amount of time you spend online speaking to strangers. Spend more time doing your hobbies, volunteering or with friends and family.	
<input type="checkbox"/> I have memory problems	Talk to one new person at a time.	
<input type="checkbox"/> I jump into things without careful judgement	Ask for someone you know and trust to go through your contacts to check if they're real. Stop - Take 5 Breaths - and Think before you click on unusual links, emails, or requests. It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you into making decisions on the spot.	
<input type="checkbox"/> I'm lonely and want more social connection	Make contact with someone you know in real life instead. There may be people around you who can help you to connect with others in your local community. Connections can also be made with people who share common interests.	

What are **RED FLAGS**?

A red flag is a warning sign of an online danger or scam.



What are Red Flags?

How would you describe **red flags** to a friend, in your own words?

Thinking back, have you seen any of these **red flags**?

Tick the ones that you've noticed:

My Red Flags

- The scammer asks me for my personal details
- The scammer asks me to send them money
- The scammer doesn't have a bank account
- Things are "too good to be true"
- Unreasonable requests
- Excuses for not videoing with me
- Broken promises for not meeting me
- Gut feeling telling me it's not right

What other red flags have you noticed?

More Red Flags...



Remember, scammers are always coming up with new and clever ways to trick us.

It is important to look out for scams even if you haven't seen these red flags.

If you are not sure, ask someone you trust.

ROMANCE SCAMS

A dating or romance scam is where a scammer tries to make you fall in love with them or become your friend.

They will take advantage of you and convince you to send them money.



Romance Scams

Thinking back, have you seen any of these **red flags** of a romance scam?

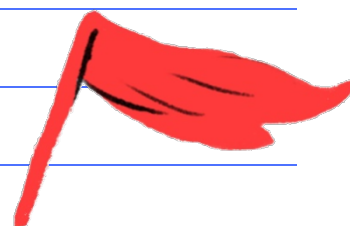
Tick the ones that you've noticed

My Romance Scam Red Flags

My Experience

- The scammer quickly says "I love you"
- You are speaking online with a stranger you've never met in real life
- The scammer's English skills are not consistent with their story
- Confusing story about why they are overseas
- The photos you receive are of different people
- Asking you to move to another site or app
- The scammer claims not to have any social media
- Broken promises and excuses

Write down your favourite romance scam story that someone has tried to trick you with:



GAINING ACCESS SCAMS

A gaining access scam is an unexpected, unfamiliar and uninvited attempt to get access to your computer, online accounts, bank details or passwords.



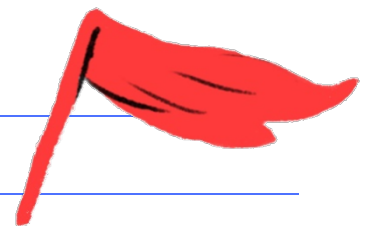
Gaining Access Scams

Thinking back, have you seen any of these **red flags** of a gaining access scam?

Tick the ones that you've noticed

My Gaining Access Scam Red Flags	My Experience
<input type="checkbox"/> I received a call out of the blue and they say they're from a large company	
<input type="checkbox"/> The number the scammer is calling from looked like it is from overseas	
<input type="checkbox"/> I didn't understand what they are saying or understand their accent	
<input type="checkbox"/> I received an email or text asking me to enter my login details	
<input type="checkbox"/> A stranger told me there is a virus or problem with my computer	
<input type="checkbox"/> A stranger asked me to buy software or sign up for an account or product I didn't ask for	
<input type="checkbox"/> A stranger asked me for my personal details	
<input type="checkbox"/> A stranger asked me to pay over the phone	
<input type="checkbox"/> A stranger asked me to pay for a bill with something other than money, e.g. gift cards, bitcoin	
<input type="checkbox"/> A stranger told me not to ask or speak with anyone else during the call	
<input type="checkbox"/> A stranger became angry when I questioned them or didn't do what they said	
<input type="checkbox"/> The scammer rushed me and told me that I needed to do things quickly	

Write down your favourite gaining access scam story that someone has tried to trick you with:



Increasing Your **CYBERABILITY**

Staying safe online is a skill which can be learnt.
There are many ways you can increase your **CYBERABILITY** (online safety)

Learn the Pro Tips for avoiding scams, find your **CYBERABILITY** lookout, and learn more about scams online.



Increasing Your CYBERABILITY

1. Pro Tips for Cybersafety

Here are some things you can do to stay safe online:

Slow down

Stay private

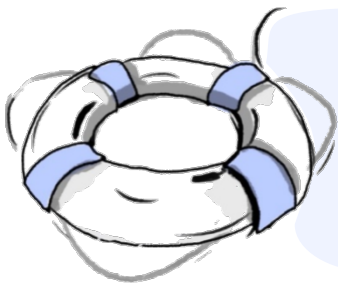
Be social media
savvy

Don't bait the
scammers

Healthy doubt

Notice the red
flags

Write here any other tips you could use to be more cyber safe:



2. Finding Your Lookout

A CYBERABILITY Lookout is someone you trust who can help you stay safe online. This could be a family member, friend, support worker, therapist, doctor, work colleague, neighbour.

Your CYBERABILITY Lookout could be someone who will:

- **Check in** with you about new apps, new people and new transactions you are making online.
- **Check out** any suspicions you have that something online is not right or if you have noticed any **red flags**.
- Have **non-judgemental** and safe conversations if you feel like something has gone wrong (e.g. unsure if the person or offer is real, you have sent money, pictures or private information to someone online who can't be trusted).
- **Help connect** you to services where you can make a report and link with the support you need.

Write down the names of the people you trust who could be your CYBERABILITY Lookout:

Which of these is most suitable? Write their name below.

My CYBERABILITY Lookout is...

- Tick this box when you have spoken to them and they have agreed to be your CYBERABILITY Lookout.

3. Extending your learning about cybersafety

Choose 1 of the extra learning links below to explore:

1 **Improve your cyberability by learning how to stay safe online:**
<https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams>

2 **E-Safety Living with disability:**
<https://www.esafety.gov.au/diverse-groups/living-with-disability>

3 **"A helpful Online Safety Guide for People with Autism Spectrum Disorder":**
<https://www.wizcase.com/blog/internet-safety-guide-for-people-with-autism-spectrum-disorders>
<https://www.autismtas.org.au/wp-content/uploads/2021/02/Online-safety-for-people-with-autism.pdf>

4 **Activity - spot a deepfake:**
<https://www.news.com.au/technology/online/fake-out-challenge-can-you-spot-a-deepfake-video/news-story/e74b98617b74757779af8ac7eccf440a>

The link I chose is...

Write down 2 new things you have learnt from the link you chose.

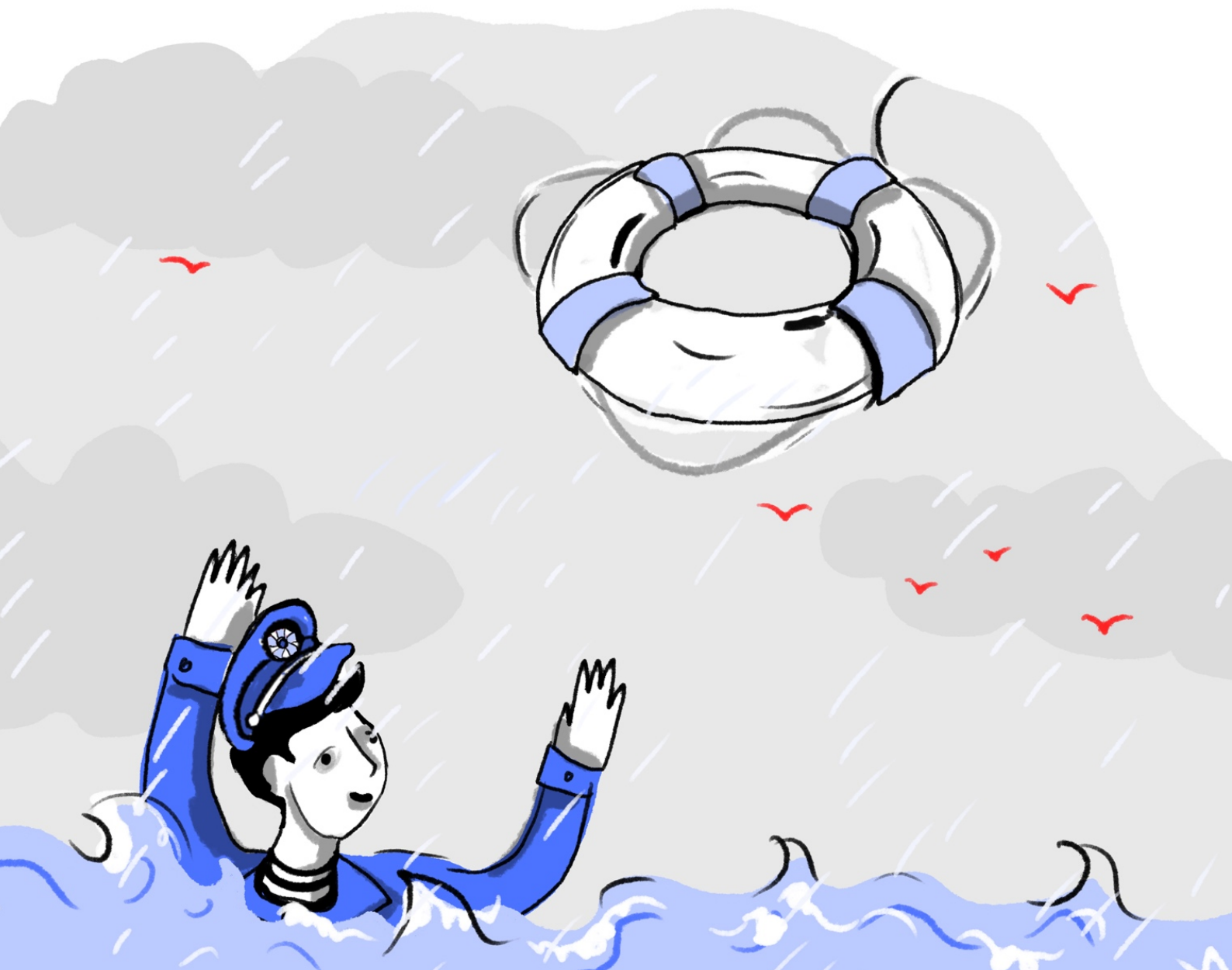
2 new things I have learnt are:

Stopping a SCAM

If you have been scammed, there are steps you can take straight away to limit the damage and protect yourself from further loss.

1. Stop contact with the scammer
2. Stop sending money
3. Reach out to someone you trust
4. Immediately contact your bank

You can also report the scam or contact a relevant service to get further help and warn others.



Stopping a Scam

Some relevant services to [report a scam](#) are:

Helpful Scam Services	How to Contact Them
<p>iDcare</p> <ul style="list-style-type: none"> • Australian identity and cyber support service. • Can help protect and support you if you have given out personal information or had your identity information misused in cybercrime. 	<p>Website: https://www.idcare.org/</p> <p>Phone number: 1300 IDCARE (432273)</p>
<p>Scamwatch</p> <ul style="list-style-type: none"> • Run by the Australian Competition and Consumer Commission (ACCC). • Helps people and businesses learn about scams. • If you have been scammed, you should report it to Scamwatch so they can inform others, monitor scam trends and take action. 	<p>Report a scam online: https://www.scamwatch.gov.au/report-a-scam</p>
<p>Police</p> <ul style="list-style-type: none"> • Can help you if you feel threatened, are in danger, or have experienced fraud and theft from the scam. 	<p>If you are in immediate danger, call 000 now. If the danger is not immediate, call your local police: 131 444</p>
<p>Australian Taxation Office (ATO)</p> <ul style="list-style-type: none"> • The only Australian service responsible for tax. • If you have received a phone call, email or text message requesting that you owe some tax, you should contact the ATO to check if this is real. • The ATO will never request that you pay money whilst you are on the phone. • If you have experienced a tax scam, you should also report this to the ATO. 	<p>If you have given personal information away or given away money, call: 1800 008 540</p> <p>If you have not given personal information away or given any money, report the scam online: https://www.ato.gov.au/reportascam/</p> <p>If you receive a suspicious email or text message, you can forward it or send a photo of it to: ReportEmailFraud@ato.gov.au</p>
<p>PayPal</p> <ul style="list-style-type: none"> • If you think your PayPal account is compromised, receive suspicious emails from PayPal, or notice any unusual charges to your PayPal account, notify PayPal to resolve this. 	<p>If you have received a suspicious PayPal email, forward it to spoof@paypal.com</p> <p>To report scam PayPal activity, go to https://www.paypal.com/disputes/ and click "Report a problem"</p>



Helpful Scam Services

How to Contact Them

Western Union

- If you have sent anyone money using Western Union and believe or find out that they are a scammer, you should call Western Union to see if the transfer can be stopped.

Call 1800 023 324

Facebook

- If you think a scammer is using a fake Facebook profile, or notice fraudulent activity such as someone selling fake items, you should report the person and/or post.

Click the “...” at the top of the post and/or profile and then click “Find support or report post”.

You can also block the person by going on their profile.

Make sure your Facebook profile is private, so only people you know can see your information.

Gumtree

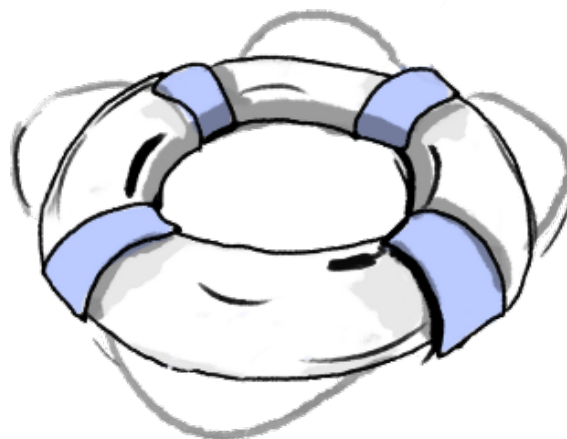
- If you believe someone is selling a fake item or have been scammed on Gumtree, it is important to report the ad so nobody else is scammed.

Click “Report Ad” which can be found at the bottom of the item’s photos

WhatsApp

- Block and report anybody on Whatsapp who is a stranger, a scammer, or contacting you from an unknown or overseas number.

Click onto the Whatsapp conversation from the person you want to block or report. Then, click on their phone number or name that appears at the top of the chat. When you scroll down, there is an option to press “Block Contact” or “Report Contact”.



Getting help from your bank

If you have given away money, or given away personal information that might give scammers access to your money (e.g. your bank account details or online banking password), you should **report it to your bank**. They can help you to close your account or change details such as your password/PIN to prevent scammers from accessing your money.

Practice finding the contact details of your bank. You can do this by searching the name and location of your bank online.

Write their details down below:

Bank name and location	Reasons to contact them	Contact details

There are other steps that you can take to report a scam or stop the scammer from contacting you. Some suggestions are below. Write down 2 or 3 more ideas:

1. Block the scammer
2. Report scams to the website or service
3. Take a break from using the online platform (Facebook, gumtree etc.)
4. _____
5. _____

Finding the Silver Lining

Not everything about going through a scam is negative.

As the saying goes, every cloud has a silver lining.

For people going through a scam,
there may be positives that come out of it.



Finding the Silver Lining

People who have been scammed had these positive take aways:

- Increasing CYBERABILITY (better online safety skills)
- Learning more about yourself and your ABI
- Learning new financial strategies
- Feeling relieved when the scam ended
- Being more comfortable asking for help
- Helping others avoid being scammed by sharing your story
- Having courage: speaking up, even if it's hard

What are some positive things you've learnt about yourself or the world when things have gone wrong?

By recognising that there can be even a small positive out of a mistake, this exercise can make us feel more comfortable with owning it when things have gone wrong, and speaking up when we need help.

Extra Support



It is understandable for you to feel a great sense of distrust, anger or distress after being scammed.

Remember to talk with people you trust about this experience and the impact it has on you.

You can also contact a counselling or support service or talk to your GP (and ask for a referral to a mental health worker).

Extra support services if you are struggling emotionally after being scammed:



Lifeline

When you need support in a crisis, contact Lifeline on 13 11 14 (24/7) or visit www.lifeline.org.au



Beyond Blue

For information about depression or anxiety, contact beyondblue on 1300 22 4636 or visit www.beyondblue.org.au



Suicide Call Back Service

Free professional telephone and online counselling for anyone affected by suicide.

[Suicide Call Back Service](http://www.suicidecallback.org.au): 1300 659 467



Kids Helpline

Telephone and online counselling and support service for young people aged between 5 and 25 years.

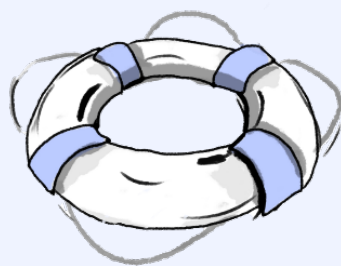
[Kids Helpline](http://www.kidshelpline.com.au): 1800 55 1800



Mens Line

Telephone and online support, information and referral service for men with family and relationship concerns. [MensLine Australia](http://www.mensline.org.au): 1300 78 99 78





CYBERABILITY

www.cyberability.org.au

#CyberAbility