Irish Examiner

LET'S TALK
ONLINE SAFETY

Littlewoods Ireland.ie

in association with

CYBER SAFE IRELAND

CYBER SAFE IRELAND

Dear parents . . .

The online world can sometimes seem like a confusing, frightening and an overwhelming place.

Good news though, it doesn't have to be! In fact, it can be an empowering and transformative environment for both children and parents alike.

You wouldn't dream of giving your child the keys to a car without teaching them to drive, and 'digital natives' or not, children and teenagers need the skills, knowledge and support to learn how to navigate the online world safely and responsibly.

The Irish Examiner, in partnership with CyberSafeIreland, and in association with Littlewoods Ireland has devised this Let's Talk Online Safety booklet to help you get started.

It's packed with advice and top tips to ensure you and your family have a positive, fun, safe and empowering experience online.

For further information and support visit:

Layout and design by Dermot Ahern, **Irish Examiner**

So what do we know?

61% of children have been contacted by a stranger in an online game

84% of kids talk to parents about online lives

87% of 8-12 year-olds have rules for going online

40% of kids aged between 8-12 are now using tiktok

13% say 'there are no rules'

93% of children aged 8-12 own their own smart device

30% have followers on social media they don't know offline

1 in 3 children have been bothered by something they have encountered while online. 22% have seen things they 'wouldn't want parents to know about'

65% of children are already on social media despite the age 13+ age restrictions set by social media platforms

31% of kids game online with strangers

All statistics are taken from Cybersafe Ireland Annual Report 2019, available on www.cybersafeireland.ie

How can you

1. Start the conversation now!
As soon as your child shows interest in your phone or tablet, talk about what's okay and not okay to do online in an age appropriate manner. Talk to your kids about what they do and see online as often as possible.

2. Do your research
Check out the apps and games that your child is using or wants to use. Download it yourself or watch videos on YouTube about it and see what functionality it has. Look, in particular, at whether it has a chat facility, how to apply safety and privacy settings and how to report abuse.

3. Agree the rules
Put appropriate boundaries in place and apply them consistently, e.g. where they can use their devices, who can be on their friends lists, what behaviour is acceptable, and not to share location. Most importantly keep an eye on what your children are doing online.

4. Build Trust
Trust works both ways. Make it clear that more trust means more freedom. If the agreement is you're going to check their devices regularly, do it in a transparent way. You don't want it to be seen as a threat so explain it in the context of wanting to support and protect them, not simply to limit their freedoms. You don't want them trying to hide problems they encounter online!

get started?

5. Establish Non-Negotiables

Boundaries are important and you need to agree 'non-negotiables' so they will apply, even when kids are not in the house. An example might be 'never meeting up with someone you met online that you don't know offline'. Practice what you preach: don't expect them to adhere to rules you don't adhere to yourself.

6. Engage

Talk to them about what they're seeing and doing online. Ask them to show you what's new, popular or trending. Play a game together. It might not be your thing, but taking an interest is an important way of building good communication and better informing yourself.

CYBER SAFETY

Staying safe on social media

More time online may mean more time on social media. Accept the reality. If your kids are active online, help them stay safer with tese simple rules.

Always set accounts to PRIVATE to have more control over shared content — most accounts are PUBLIC by default.

Keep an eye on “Friends’ lists — made sure that permission must be requested to ‘follow’ or ‘friend’ the account.

Be careful to not overshare in the profile by giving away your image or too much personal information.

Turn OFF ‘Location Settings” – this prevents posts or photos and videos being geotagged and protects you location.

Avoid clicking on targeted ads and giveaway offers — these can be scams or lead to inappropriate contact.

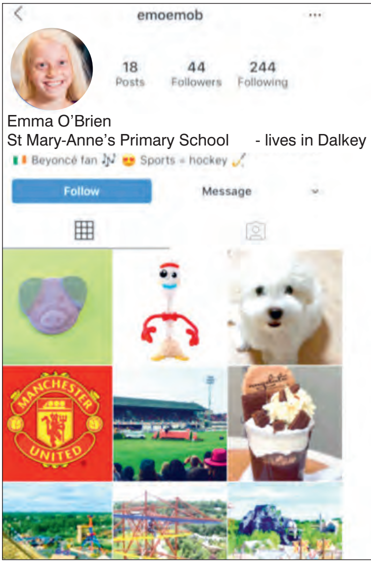
Creating safe profiles

- What not to have on social media profiles
    - ➤ school crest
    - ➤ face pictures
    - ➤ telephone number
    - ➤ location
    - ➤ personally identifiable information

- Settings - the default setting is usually public so make your account **PRIVATE.**

- Understand the difference between Friends (people we probably know offline) & Followers (who could be anyone anywhere).

- Understand the difference between 'following and followers' — it's ok to follow lots of people, but not necessarily have them follow you!

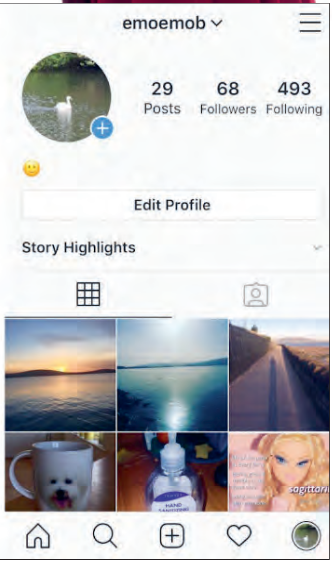


emoemob

18 Posts 44 Followers 244 Following

Emma O'Brien
St Mary-Anne's Primary School - lives in Dalkey
Beyoncé fan 🎶 😍 Sports = hockey ✓

How is Emma's profile safer now?



emoemob

29 Posts 68 Followers 493 Following

🙂

Social Media Settings

Social media platforms often by default have access to your location — so switch location settings **OFF**

Restrict the app access to microphone, devices contact list, camera and location

Make the account private - by default social media accounts are usually set to public - meaning anyone in the world can see what the account holder is posting, their comments, likes and stories.

Allow some apps access to location is ok! e.g. Google Maps or the local weather

Establish rules of who can be followed, whether your child can allow followers, and who those people should be

Create a Close friends or Supervised friends list - it is a good idea to keep a close eye on your children's friends list: ask them to think about what they are sharing with whom

Social Media Posting

- Weigh up the benefits and risks of sharing the information or image first - how will it affect me or others?

- Am I giving away too much personal information or putting myself or others at risk?

- Ask yourself . . .
Is what I am posting a true and a real representation?

- Anything you post can be screenshotted, downloaded or reshared - deleting it does not mean it has gone from the internet either

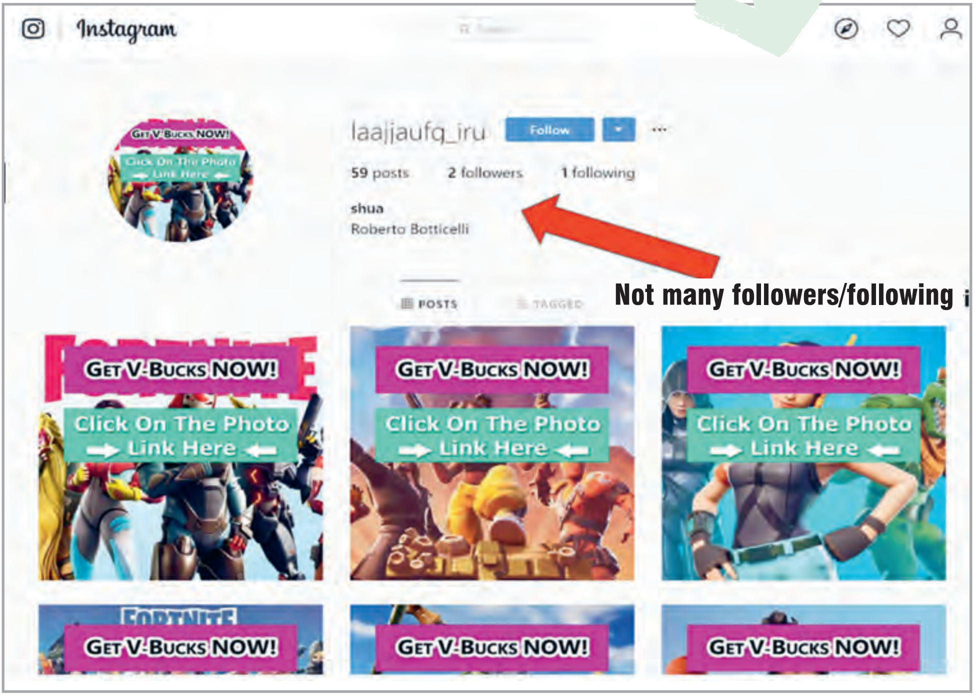
- Whatever you post will become part of your digital footprint

- Will I be proud of what I am posting or sharing in 5 years?

Always think **BEFORE** you post

Social Media Scams

This an example of a social media account created purely for scamming



laajjaufq_iru

59 posts 2 followers 1 following

shua
Roberto Botticelli

Not many followers/following

- Look for tell-tale signs e.g. All posts on the page the same image, few or no followers/following, computer generated name, offers something free
- Wants to be clicked on - do not click the link as you cannot trust the source
- Do not add these accounts as followers these accounts
- Do not accept invitations to join group or follow

Live Streaming or Uploading Video Content

THINK: what is in your background? Do I want to share this also?

THINK: who is in your background? Does this person want to be filmed? Do I have their permission?

Always remember someone can be recording or screenshotting what you stream or post

Whatever you share can always be out there somewhere. You can't control what others do with your content.

Make sure streaming has ended and you have switched off access to your camera or closed the app properly

If you're making and uploading videos only use copyright-free or public domain images and music: always give attribution credit to the creators.

Smart Device upkeep

- Have a secure passcode on your device.
- Change factory default passwords.
- Never connect to free public wifi - this is usually not secure.
- Keep your device software up to date - but remember always double check privacy settings after an update, as some of these can change.
- Update apps regularly and offload any expired apps or ones that you don't use.
- Cover the camera on your devices when not in use . . .

Covering a computer's camera doesn't protect the device from being hacked, but does prevent a hacker from being able to see whatever the camera sees.

- Disable your microphone access for most apps or cover to muffle the audio enough to prevent a hacker from listening in, uninvited.

Safety settings

Use Parental Admin platforms

Google Family Link or Apple Family Sharing will give you more control to monitor activity and content on children's devices through your own.

In-app purchasing

Some apps downloaded on smartphones may include in-app purchases, so you may need bank card details added to accounts.

Passwords

Help your child to create strong passwords: an easy to remember mixture of letters, numbers and symbols is the toughest to crack!

Passcodes and Pin Devices

Make sure these are in use and are sensible choices, not 1234 for example!

Have rules on smart device use: where, when and how can they be used?

Make sure to **install software updates** and teach your child the importance of this.

Disable location services

Maps and weather are the only apps that need access to the devices location.

Online gaming

Our gaming house rules

With gaming redefining how young people socialise, try our gaming guru Olwyn's suggested house rules for a smoother family gaming environment.

1
Who you friend

Only play with offline friends, never with strangers.

2
In-game behaviour

Be kind, be inclusive, report toxic behaviour.

3
Game Suitability

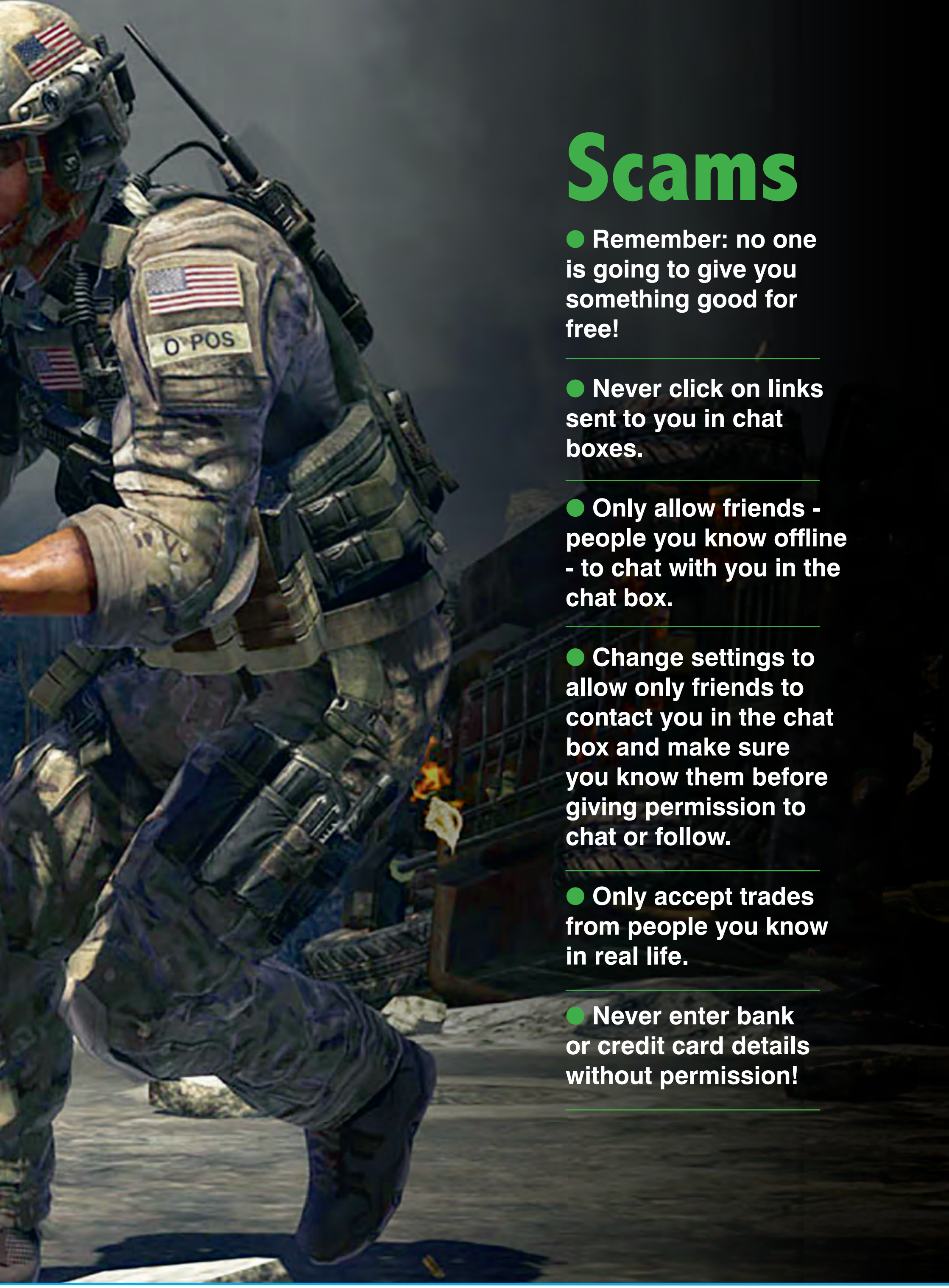
Check content and age rating on the PEGI website.

4
Time spent

Avoid single sittings and spread game time across the day and different games.

5
In-game spending

Keep purchases for special occasions like birthdays.

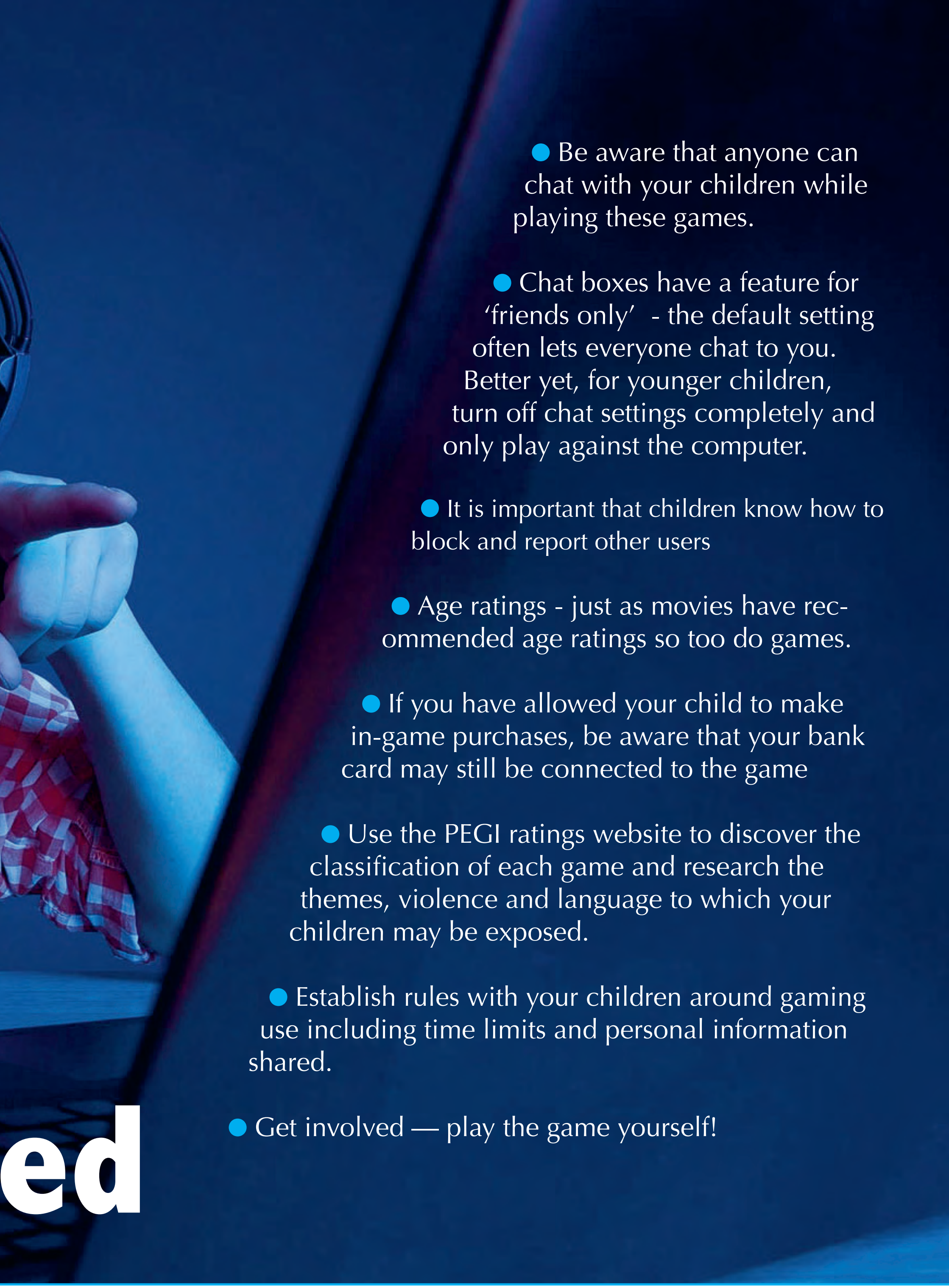


Scams

- Remember: no one is going to give you something good for free!
- Never click on links sent to you in chat boxes.
- Only allow friends - people you know offline - to chat with you in the chat box.
- Change settings to allow only friends to contact you in the chat box and make sure you know them before giving permission to chat or follow.
- Only accept trades from people you know in real life.
- Never enter bank or credit card details without permission!

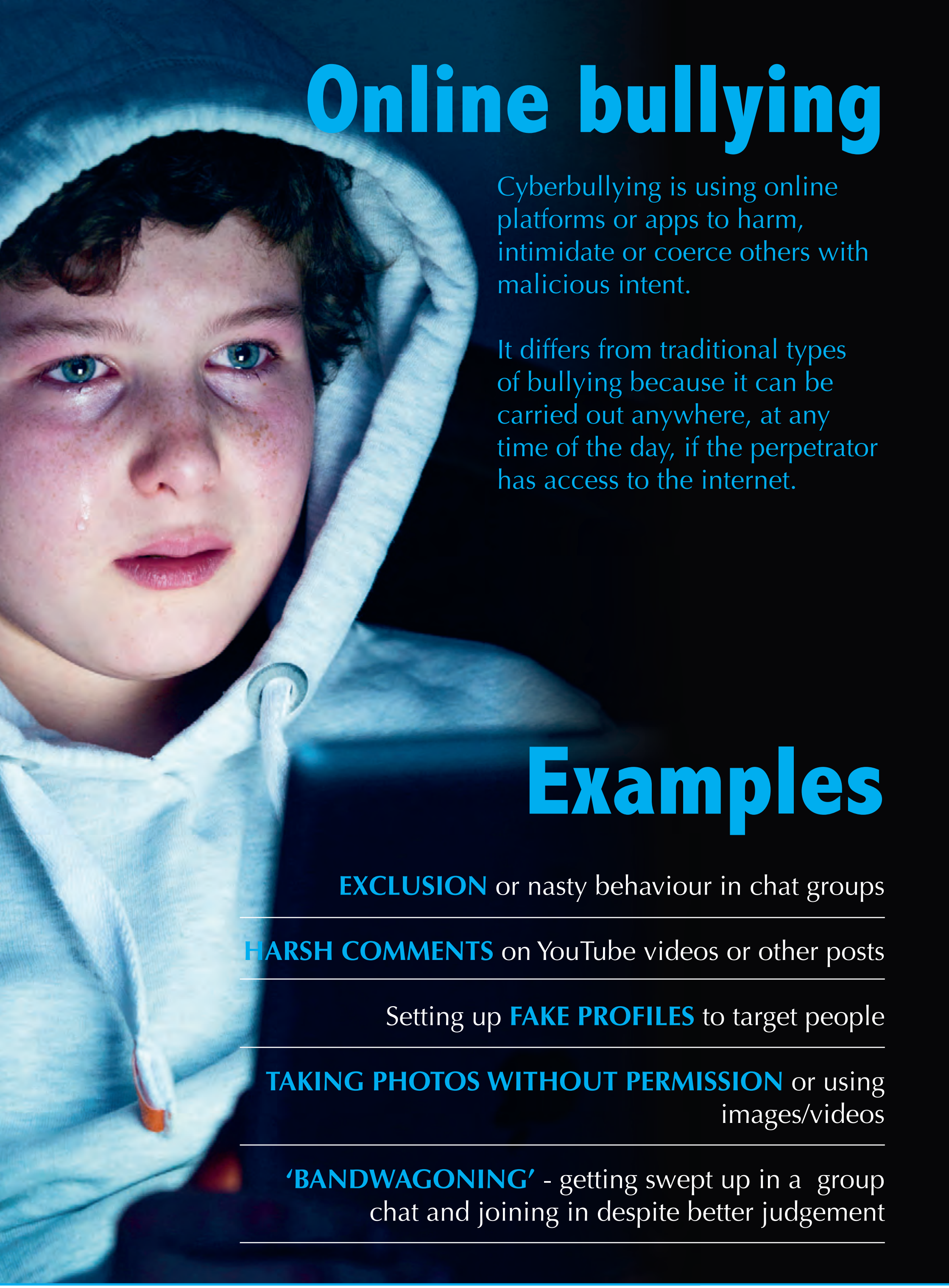
Inform yourself . . .

. . . get involv



- Be aware that anyone can chat with your children while playing these games.
- Chat boxes have a feature for 'friends only' - the default setting often lets everyone chat to you. Better yet, for younger children, turn off chat settings completely and only play against the computer.
- It is important that children know how to block and report other users
- Age ratings - just as movies have recommended age ratings so too do games.
- If you have allowed your child to make in-game purchases, be aware that your bank card may still be connected to the game
- Use the PEGI ratings website to discover the classification of each game and research the themes, violence and language to which your children may be exposed.
- Establish rules with your children around gaming use including time limits and personal information shared.
- Get involved — play the game yourself!

ed



Online bullying

Cyberbullying is using online platforms or apps to harm, intimidate or coerce others with malicious intent.

It differs from traditional types of bullying because it can be carried out anywhere, at any time of the day, if the perpetrator has access to the internet.

Examples

EXCLUSION or nasty behaviour in chat groups

HARSH COMMENTS on YouTube videos or other posts

Setting up **FAKE PROFILES** to target people

TAKING PHOTOS WITHOUT PERMISSION or using images/videos

'BANDWAGONING' - getting swept up in a group chat and joining in despite better judgement

Things to look out for

Some of the most common symptoms of cyberbullying or being cyberbullied are:

Withdrawn from friends or family

Sadness, frustration or anger when online

Sadness, frustration or anger after being online

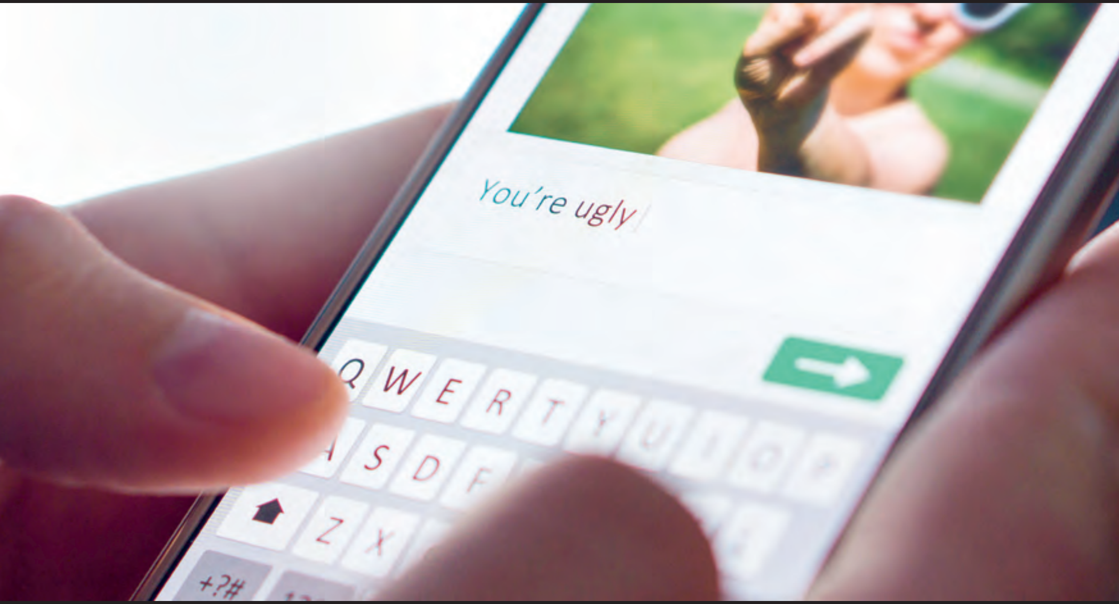
Unusually secretive about online activity

Decline in school work or interest in clubs & activities

Changes in friendship groups

Changes in sleeping habits

Dealing with cyberbullying



Whether your child is cyberbullied or is cyberbullying ...

Stay calm, respond positively and reassure them. Encourage them to talk openly and discuss options

Advise that they don't respond or delete – screenshot for evidence

Use online blocking & reporting mechanisms

Check out privacy settings on their online accounts

Talk to the child's school, and the Gardai if involving serious harassment, threat of harm or indecent images or videos

Link or stink . . .

There is no such thing as 'free' even if there was, you wouldn't have to hand over your login details or card details… so don't give these out if in doubt!

Do some detective work if you are in any way sceptical (which you always should be of everything online). Take the time and look for cues: these are not always apparent at first glimpse.

If you receive an unsolicited email check the sender address, especially if it came by text - you can also google to check if things like this have been scams previously. It may seem from a reputable company but check the actual address.

Look at the link before you click. If anything looks wrong, it probably IS wrong. Even if the scammers don't make any spelling or grammatical mistakes they almost always need to lead you to a website that they control. Often, that means a bogus link that you ought to spot if you take your time. Never let yourself get rushed into clicking through, no matter how much the scammers play on your fear of missing out.

Staying safe on video calls

For stronger, smarter and safer communication

Turn off additional features such as private chat and sharing files

Use private passwords and virtual ‘waiting room’ for better control and to prevent ‘bombing’

Never share any personal info in a Zoom meeting

Beware of phishing links: is it really a Zoom invite?

Report any issues directly to Zoom

Keep your version updated regularly

VIDEO CALL ETIQUETTE

Having a cover for camera is a good idea - you can either use a post it or bit of tape or buy a sliding webcam cover

It is important to know how to turn camera and microphone features off on the platform you are using (they all differ). A quick search on Google or YouTube will show you how!

Know who you are talking to or who your are letting join (create a registration link).

If you are setting up the conference call or webinar, have a password.

NEVER share personal information on video call especially on the chat feature.

Use a virtual background or plain wall or space in your house.

Always be aware someone can be recording or screenshotting your calls.

If you are sharing your screen, have the tabs open and ready to share - this limits access to private information or inadvertently embarrassing pictures!

Keep pets in another room - especially if it is a work call or serious meeting!

Sexting

Sexting is sending sexually explicit photographs or messages via mobile phone. Ireland has one of the highest teen sexting rates in Europe.

88% of sexually explicit self-generated images end up somewhere on the Internet, even if they are sent privately originally

Explicit image/video of a child could be an offence under Child Pornography legislation: don't screenshot, share or delete these images

The emphasis should always be on containing the image/ video as much as possible and supporting the child

Contact the Gardaí for further advice on how best to proceed

Remember that curiosity about sex, sexuality and their appropriate expression are normal parts of young people's development

It's important to establish the difference between consensual and non-consensual explicit image sharing in terms of understanding how best to approach the problem when it does arise.

Digital footprint

A digital footprint is the trail we leave behind us online and is very hard to erase. Almost everything we do online adds another piece to our digital footprint, so it's essential to try and make it as positive an imprint as impossible!

Keeping it positive

THINK before you click 'Send'

Be **KIND** to others, show **EMPATHY**

Don't **OVERSHARE**

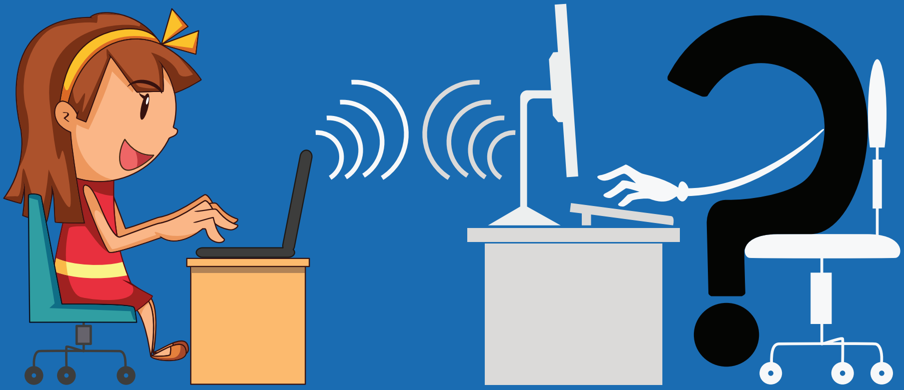
Try not to **BANDWAGON**

Don't **RESPOND** to cyberbullies or people you don't know

REMEMBER what you post online stays online

Google yourself: would you be **PROUD** if someone else did?

How to spot fake information online



More time online means more exposure. We're creatures of habit, but try to vary your sources and watch for fakes

NEWS

Beware of Forwards! Did it originate on social media or is it from a reputable new source? Finding the same story in at least two or theree trusted places will help test it veracity.

ACCOUNTS

Not all accoounts are real and many are 'bots', designed to troll people, generate likes, comments and followers or take over accounts automatically — they aren't real people!

INFLUENCERS

There are lots of influencers and models on social media like Miquela or the Balmain Army, designed by companies using AI technology. They look real, they feel real, but they're not!

E-MAILS

It might look real, but check the address. Does it use your name or just 'Dear Customer'? Poor *grammer* and *spelin* are also a giveaway that it's probably fake.

DEEP FAKES

AI technology can take existing video and mimic the speech patters to get famous people to make unexpected or false statements. They look very real, don't be fooled.

Don’t get Phished

1. Check the email address, even if it’s a company you trust

2. Change password regularly – make them strong

3. Watch out for vague terms like ‘Dear Customer’

4. Be suspicious of odd grammar and spelling

5. Never open unsolicited attachments

6. Beware of e-mail or app ‘forwards’

7. Hover over links to see the sources

top 10 tips

for staying SMART and SAFE online

www.cybersafeireland.org

1

Visit our website for more information, advice and resources

In light of the current Covid-19 crisis in Ireland, we will continue the even more vital work of promoting online safety by moving our training sessions online.

Click for more information

What we offer

2

Switch off **location settings** and understand the dangers of **geotagging** posts

3

Do things **together** online

4

Discuss the importance of **personal information** and dangers of oversharing

5

Use **parental controls** and **filters** at home and on devices

6

Discuss the diffrence between **friends** and **followers**

7

Try **‘device-free’ dinners** and **model the behaviour yourself**

8

Do your **research on** popular apps and games

9

Talk about the **positives** and **negatives** of being online

10

Have a **device bedtime** that's earlier than your kids bedtime

Irish Examiner

DELIVERED TO YOUR HOME FOR FREE

Irish Examiner
Wild west
Turning the tide
Opening night
€200m fund to reopen schools
Fenced off for the future
Competition
New look Weekend
'I want to see Ireland as an example to men and women everywhere of what can be achieved by living for ideals, rather than fighting for them, and by viewing each and every person as worthy of respect and honour.'
John Hume, 1937-2020
I do – but how?
Modern marvel
Class distinction
Gun and its story
Flat footed
Bok with a bang
Outrage at one law for them, one law for us

FREE HOME DELIVERY SERVICE - SIGN UP TODAY

Contact us today to sign up for any of the packages below, or to get further information.
www.newsdelivery.ie | 021 430 00 28 | info@newsdelivery.ie

€52 Per month
Save over €300 per annum

EVERY DAY BUNDLE

The Irish Examiner delivered to your home every day Monday to Saturday plus daily ePaper access.

€22 Per month
Save over €70 per annum

SATURDAY BUNDLE

The Saturday edition of the Irish Examiner delivered to your home plus daily ePaper access.

Just pay the cover price

ANY DAY DELIVERY

The Irish Examiner delivered to your home on your chosen days of the week.