SOCIAL MEDIA

USER SAFETY GUIDE

Last year the Garda National Cyber Crime Bureau (GNCCB) was pleased to publish our ***Cybercrime Risks & Prevention Tips*** booklet that documented the online crimes affecting electronic device users on a daily basis and the steps that can be taken to *Keep Safe Online.* This second booklet, Social Media: User Safety Guide, is intended to provide readers with insight into the social media environment, and the steps that can be taken by you, as a user of such services, to *Keep Safe Online.*

As I said in the past, the internet and the instantaneous global connectivity it creates has had a hugely positive impact on societal and industrial development. Advances in our technology and the ease at which communication is now possible has revolutionised how we interact. However, along with the many transformational benefits, there are many dangers. This is also a reality within the social media environment.

Social media enables us, as users, to upload and share a myriad of personal and sensitive information. Prior to the advent of social media, much of this was information that we would have ordinarily kept to ourselves or made available in a much more guarded way. We would rarely have considered openly advertising our personal preferences, addresses, holiday intentions or images and videos on platforms where they can then become available for all the world to see. However, this is the reality with many social media postings we upload, whether such availability is intended or not. It is also very often the reality that once online, such material can be very difficult to remove.

The ability to gain intimate knowledge of a person or organisation can often be exploited by criminals. All of this online information can become available to cybercriminals who use the same data to tailor their criminal enterprise in a manner that provides them with the greatest opportunity of being successful in their illegal endeavour.

The reality is that these criminal actors operate on a global scale and many are highly organised. The threat they pose should never be underestimated; neither should the harmful impact that frequently results if you are a victim of cybercriminality. It is important that every action you, as a social media user, take retains at least some degree of cognisance of the fact that no-one is immune to being targeted if criminals are presented with an opportunity to strike.

One of the Garda National Cyber Crime Bureau's most critical roles is promoting the importance of combating the harm caused by cybercriminality through preventing it from occurring. This latest publication continues the ambition of GNCCB to support you, the public and business communities, in preventing cybercriminality and social media abuse by creating awareness and offering advice on how to best navigate through the existential risks that are the reality of our lives online.

Social Media is now a very important part of many of our everyday online lives. It is our intention that as a result of this booklet you, the reader, will be able to recognise and proactively take the most important preventative actions that will enable you to fully enjoy the positive benefits of social media while Keeping Safe Online.

Barry Walsh
Detective Chief Superintendent
Garda National Cyber Crime Bureau

Let's talk about Social Media

> *The first rule of social media is that everything changes all the time. What won't change is the community's desire to network*

Social media helps us to chat or send content at the push of a button to another country or even another time zone. Its arrival revolutionised our communications but also opened us to a new world where instant abuse is possible. This guide is designed to help make social media a safe space for all its users. It can only be effective as a support where social media users take appropriate personal precautions when going online.

Before delving, in detail into social media and the rules of *#KeepingSafeOnline,* the following is a high level overview of some of the common questions that this booklet will seek to answer.

What is social media?

Most people know the names of the main social media platforms and how to use them. But what exactly is social media and how does it actually work? We take a quick look at the back-office workings of online communication.

What types of social media exist?

Many people use chat forums or online platforms to socialise online but what are the types of social media that exist and what does each offer?

What are their rules of engagement?

Most social media platforms set rules about using their services, but what are they and are they very different? Equally important is whether they are enforced or not and by whom!

What types of crime occur on social media?

While the vast majority of our interactions on social media are positive, they can go very wrong. We take a look at some of the crimes that can occur and how they are enabled by online platforms.

How can I avoid becoming a victim?

Is it possible to avoid becoming a victim of social media enabled crime and what are the basic rules to stay protected as you chat and share online?

5.2 Million
Mobile phone connects in Ireland.

80%
of social media spread across the population

55% female users **45%** male users

Social Networking platforms like *Facebook* and *Snapchat* focus on person-to-person conversations but also facilitate content and knowledge sharing. Users can create content and groups but the primary focus is the social element of connecting online.

Video Streaming and sharing sites like *TikTok* or *YouTube* provide a platform for uploading and viewing video content on any subject. Users with enough followers can also earn revenue through ads on their own dedicated channel.

Discussion forums such as *WhatsApp* or *Reddit* give a venue to ask questions and get answers on shared interests or topics of interest. They can also be used for research and customer surveys. Image based sites such as Pinterest and Snapchat focus on sharing images or quick posts that send a message but are not intended for long conversations.

Finally blogs and community forums like Tumblr or Blogspot allow likeminded users to engage on a common topic and converse or exchange as much or as little as they like on the theme. Most social media companies now offer an Artificial Intelligence (AI) component as standard.

What is social media?

There are a number of definitions of what social media is but it's often described as digital technology that allows users to share content and information such as text, images, ideas and conversations over varying dedicated platforms, virtual networks and communities. The content can be downloaded from another site or page, or it can be self-created by the user. You can interact with friends and unknowns, and many businesses have social media accounts that are used to market their products and services to a wider customer base than would be available to them if they advertised only offline.

The term 'social' comes from the fact that the platforms are designed to put users in social contact with each other but what differentiates one platform from another is the type of content being shared.

Social media serves a clear purpose of putting people in touch with each other whether it is likeminded users or potential customers. While most platforms have rules that govern who can join and what you can post, the reality is that there is relative freedom on the content that users put on their accounts and a large proportion of posts are reshared across multiple platforms by users who have accounts on each. The rule is, in advance of posting online, you should very carefully consider what you put on public facing social media as it has the potential to remain online for ever more. That consideration should be towards yourself and other online users.

What user rules apply?

All social media platforms have clearly defined rules of engagement that govern who can join and what can be posted to their platforms, or equally what should not be posted. There are behavioural rules that social media platforms apply regardless of which platform you use and they require users to behave in an ethical and appropriate manner. Criminal and personal issues often arise where these ethical or behavioural standards are disregarded.

When it comes to putting content online on any platform, consider if you would make the comment to someone in person; would you hand over a physical copy of the image you are uploading to another person and let them take it away; or finally would you be comfortable seeing the material posted on a notice board in your local shop, club, workplace and school? If the answer to any of these is no, then don't post it online for the world to see.

While every social media site sets rules that differ, depending on the platform, all of them prohibit the upload of sexual, violent or copyrighted material, or illegal acts and products to their forums.

What differentiates most of them, is the minimum age they require their users to be before joining. The majority of social media platforms permit users who are 13 years of age or older but some such as Spotify or YouTube require parental permission if under 18 years. Others such as Flickr restrict access to some materials where the user is under 18 but permit the user to have a personal account.

The difficulty that arises with age restrictions on social media is that in most cases the user is only asked to confirm they are over the age but are not required to provide any proof of age other than a date of birth. Some platforms have introduced policies where they estimate the user's age based on their profile activity while others require some form of identification verification but this is the exception rather than the rule.

There have also been calls to use facial recognition technology to estimate a user's age using known ageing parameters but the reality is that many users have not reached the age required and have accounts on sites that may not be suitable for them to use.

The reality is that social media is by its nature a free and easily accessed form of both expression and communication with limited controls other than those around illegal content or where the user responsibly monitors their own activity and/or the activities of the child they have responsibility for. It is worth noting that the terms and conditions of many social media platforms ensure the user owns their content. However, these agreements usually look for the user's consent to access and use their content and images which the platforms often need to sustain their own respective business models, including sharing it with external third parties. The general rule is that in an online environment, if you are not paying extra for the service, you are the product and part of the business model employed by social media providers to sell their own service. Most users are comfortable with this but it is important that users are aware of the need to read and understand every platform's terms and conditions of use before joining up.

Age of Use for Social Media Platforms

X (Twitter) Facebook Instagram Youtube TikTok Snapchat WeChat Pinterest	Kik Flickr LinkedIn Path	Tinder
13+	16	18

S Any sharing of content must be responsible and appropriate.

O Obey the rules and guidelines of the platform or forum you are using at all times.

C Copyright protections & property rights must be respected when posting online.

C Constructive communication & comments in all interactions with other users.

O No objectionable, violent, or sexual content should be posted to forums or pages.

R Rules aroud privacy and data protection must be adhered to at all times.

What crimes occur?

Whether it is cyberbullying or online frauds, the internet and Social Media provides a platform where almost every crime can occur or have its origins. Its remoteness and virtual nature gives online users a false sense of security and protection, while providing criminals with a high degree of anonymity which can make it difficult for potential victims to identify the activity as a potential threat. The reality is that we are more vulnerable online for those very same reasons in that we are more accessible and easier to abuse than if we were face-to-face with a potential attacker.

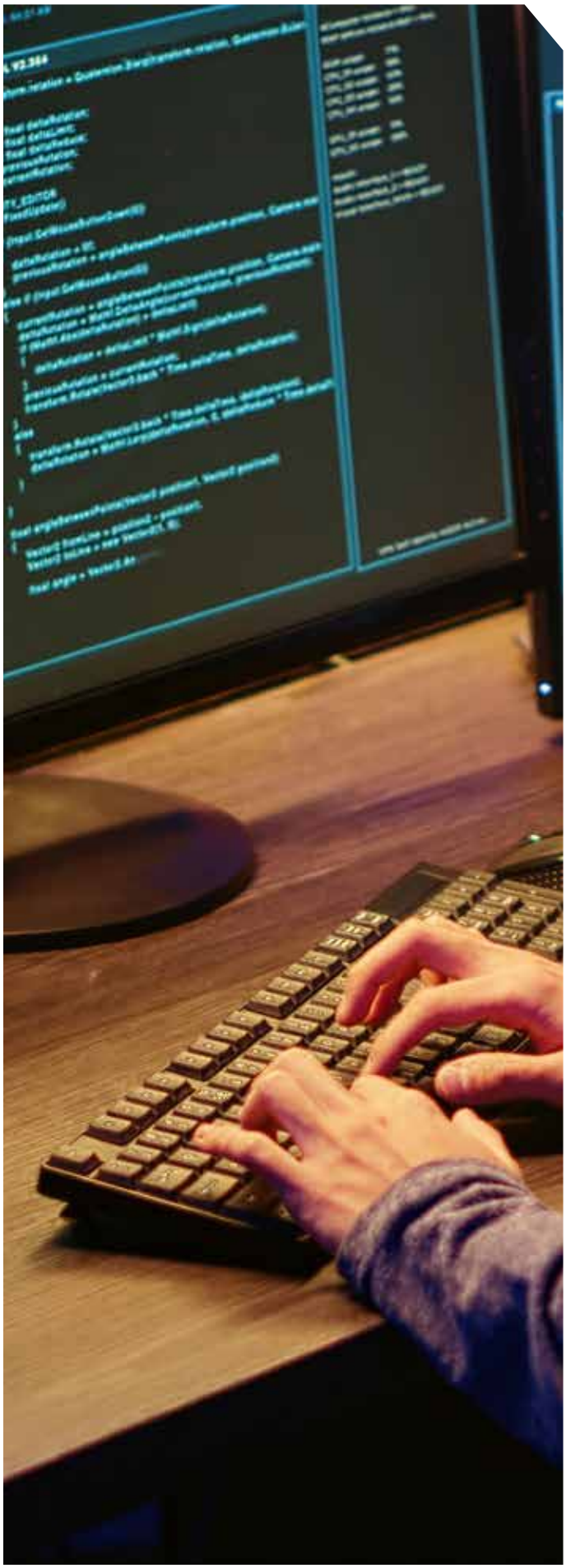
Online Sexual Exploitation

This type of online crime can occur over social media where the child will typically receive a friend request on social media from someone posing as another child, often with a profile that has been faked using copied images and content from the Internet. Once trust has been built, the abuser 'innocently' suggests they exchange naked images for fun.

Once their victim has sent nudes, the abuser reveals who they really are and threatens to tell family and friends if the child doesn't send more images or pay them to keep silent. All of these are crimes under the Criminal Law (Sexual Offences) Act 2017 (sexual exploitation), the Criminal Justice (Public Order) Act 1994 (blackmail) and where naked images of a child are traded, the offence of producing Child Sexual Abuse Material (CSAM under the Child Trafficking & Pornography Act 1998 occurs).

Online Exploitation

While the Internet gives access to a wide range of content, it is also a platform on which abusive or violent content is shared and traded. Many of these content sharing groups are private. You must share share CSAM content to be admitted or to start trading. At the same time, the content can be violent or easily shared over social media, encrypted apps or private groups and the darknet. This includes content that is shared by online groups that use exploitation and bribery to radicalise children into committing acts of violence themselves which could be an offence of coercion under the Criminal Justice (Non-Fatal Offences Against the Person) Act 1998.



What to look out for

Out-of-the-blue friend request from someone who claims to know you or be the same age.

The profile is recent or has very few mutual connections, if any at all.

Someone suggesting they are a friend and being overly friendly with you or praising you.

A profile pic that shows a very attractive person or that is overtly sexual in content.

Receiving links or attachments that show violent content from someone you don't know Invitations to groups on the darknet or that are encrypted and offer violent or illegal content.

A change in mood or personality that is sudden or progressively gets worse over a short time.

Children who suddenly become very secretive, confrontational or hyper-critical about others.

Cyberbullying

Children of all ages have constant access to devices and the internet so it should be no surprise that online bullying is now a regular occurrence and a constant threat for social media users. Many children are confronted with abusive content that can affect their personality or their performance at school. Ridicule and threats can be sent by individuals or a group acting together, often at the instigation of one main offenders.

Examples of this form of abuse include directing abusive comments to someone, impersonating another person and posting negative content that appears to be coming from them, or sending private images that were shared with the expectation that they would stay within a select group.

Regardless of the form that it takes, online bullying or harassment is a crime under the Criminal Justice (Non-Fatal Offences Against the Person) Act 1998.

Cyber Stalking

Like most offline crime, the crime of stalking has migrated to social media with people being put in fear that they, or their close friends and family, will be attacked by some faceless abuser online. Like its bullying cousin, stalking causes such alarm or distress to the victim that it has an impact on their life because of the fixated, mostly unwanted and repeated attention they receive.

Cyber Stalking can take the form of repeated and increasingly aggressive social media posts that often start with an expression of affection or dependence. It can be someone who obsessively comments on your posts or tags you in their own. Online stalking can emerge when another user shares your personal information with other people and gives the impression that they have your permission as a close friend. Stalking amounts to a crime under the Criminal Justice (Miscellaneous Provisions) Act 2023 and, like all crimes, should be reported to Gardaí.

What to look out for

Multiple negative or critical comments about you or someone you know, or about your posts, ability or your online profile.

Unwanted chats or requests from someone you don't or barely know but claims to be a friend.

Frequent comments on your posts or on the posts of others about you, whether critical or not.

Friends that suddenly stop talking or chatting with you online or avoid you without explanation.

Sexting

An ongoing phenomenon amongst young people and children is to share sexual images of themselves among their friends. While this may appear to be a harmless act, the reality is that many of these images are shared outside those groups or naively shared with someone else outside the group in the belief that the other person on social media is another child or someone the sharer knows. In many cases, this third party is an adult impersonating a friend or another child. Sharing images of a naked child is an offence under the Child Trafficking & Pornography Act 1998, regardless of the age of the person who shares.

Revenge Pornography

The term revenge pornography encompasses any form of naked image of a person that is taken with consent or without their knowledge even if they were the person taking the image and where that image is then shared as a form of punishment. This crime occurs when these private images are shared without consent, online or by any means by the subject's partner or former partner, with the intention of causing distress or harm or being reckless about the possibility that harm may occur.

The victim does not have to be naked as images or content which show a person in underwear can also fall foul of the law in Ireland if harm is caused or could be caused. Sharing intimate images of another person is an offence under the Harassment, Harmful Communications and Related Offences Act 2020.

What to look out for

Sexualised comments about their friends, peers, partner or others that are out of character.

A child or adult who becomes very secretive or private about the images on their phone or computer.

Spending more time alone in their room than usual or leaving the room to talk or message.

Sexting may lead to the sudden loss of a friend without explanation or avoiding a friend for no apparent reason.

Revenge pornography offences usually lead to someone telling the victim they found images.

Deepfakes & Online Frauds

In simple terms, a deepfake is where an image, video or voice message has been manipulated with technology, often AI, to appear to be something or someone else. Very often, they are created to enable a fraud to be committed by fooling another person to send money or their personal data, to accept a friend request on social media or to help a charitable cause and are used in the following crimes:

Romance Scams

The lure of romance is enticing. The amount of romance sites and social media platforms offers potential partners of all varieties and situations. Posts on social media platforms can be seen by fraudsters looking for vulnerable or lonely victims to exploit for their money. Typically, these crimes start off with a scammer connecting with another user on social media and using the offer of romance, praise and flattery to eventually win their victim's trust.

Conversations turn to romance but the fraudster never reveals anything about themselves and steadfastly refuses to meet. Quickly they claim that they need money to fund an operation, a business venture or to travel and meet their new love. The sums can start small or can be a large 'sign of how much they are in love'. However, it's all a social media con and an offence of deception under Section 6 of the Criminal Justice (Theft & Fraud Offences) Act 2001.

What to look out for

Did you recently post on social media that you were looking for romance and the message with an offer of romance followed very quickly after?

Is the person very attractive or even too good to be true or are they very obviously what you are looking for?

Have they asked you lots of questions about yourself but shared little about themselves? Have they made excuses when you ask to meet or are they evasive about their background?

Have they asked you for money to fund a medical treatment or business venture or to travel and meet you, and asked you to send the funds using money transfer, rather than via a bank?

Fake Job Offers

Many people use social media to find their dream job or students post to social media accounts for summer positions that will provide them with an income to fund their next year in college, their summertime activities or the holiday they want to take before they return to study.

Fake job offers have all the hallmarks of real jobs but the difference is that they often appear after a person posts that they are seeking employment. They are designed to steal personal information about the applicant or trick them into sharing banking details over the fake job application platform or with the other party directly. This includes a job where you are asked to lodge money to your account in return for a fee, which is called 'money muling' and is a crime as it involves moving illegally-gained funds through real accounts to launder it.

What to look out for

Did you recently post online that you were looking for a job and this offer popped up soon after?

Is the job perfect for your needs or is the offer very vague about what it involves?

Have they asked for personal or banking information before offering you the job?

Did they offer you the position very quickly without a proper interview or checks?

Have they pressured you to give them an answer quickly?

Can you find clear information about the company or recruiter online?

Delivery scam

Part of the process of ordering goods and products online is the email from the supplier telling you that the package is on the way or will be delivered in a few days. The new way of scamming customers is to send a message or a link saying that the package is delayed or stuck in customs because a processing fee has to be paid.

The message has all the hallmarks and symbols you would expect from a reputable delivery service and it can be either an email or a text message, using the details that we often post to our social media accounts.

Toll Payment Scam

Another popular scam is the one telling us that we have failed to pay the toll for using the motorway in recent weeks. The message tells us that if we don't pay up, the fine will continue to increase and we could even be summonsed to appear in court. The scam preys on the fear it generates and targets our pockets with the threat that failing to respond will cost us money.

As with all of these types of scams, the email looks genuine with the logos and email address you would expect to see, but the tone is threatening and urgent and instructs you to click on a link to make the appropriate payment, or else!

Lottery Scams

Most people dream of winning the lottery. The prospect of not having to work is very enticing as is the idea of being able to buy whatever you want without having to worry about budgets or the bills that have to be paid.

A number of varieties of this scam exist. You may receive a message from the lottery saying you should click on the link to claim your prize. Alternatively you receive a message stating that you are the beneficiary of a political leader's stolen funds and need to give your contact details to receive the funds, what is known as a 419 Scam letter.

Fake "Send-me-money " scams

When children go on holiday alone or with friends, their parents invariably worry that they are ok and will return safe and well. At the same time, it is not unusual for a child to run out of money while away with friends and a request to deposit funds in a bank account wouldn't be unexpected. Cybercriminals are aware of this and will send a message that appears to come from a child saying they have been mugged and all their property stolen. Often the message is accompanied by a photo of the child appearing injured. In these cases AI has been used to manipulate a photo downloaded from your child's social media account.

What to look out for

- Did you order goods that you expect to be delivered or purchase a ticket for the lottery you won?
- Have you recently passed through a toll road without paying - say in the last week?
- Is there a phone number on the message you received about the package, big win or missed payment?
- Do you recognise the number the message has been sent from ?
- If the answer to any of the above is no - beware and think twice before responding.
- Can you contact your son or daughter directly to verify they are ok and that the message is true?

What are the signs of abuse?

Knowing the risks that exist online and how they can manifest as crimes is the first part of the process of protecting yourself and others from online abuse. The next step in the process is being able to recognise the signs that abuse has taken place which will enable you to respond and support the victim, and help them to both recover and stop the abuse from continuing.

In most cases where social media abuse takes place, the victim has been threatened to keep quiet or is afraid to say anything in case the abuse gets worse, or the attacks will move from online to physical harm. There are a number of signs that can indicate that your child is being abused or bullied online.

At the heart of all of these is establishing trust with your child so they know what social media abuse is and so they are comfortable telling you when it occurs or when they don't feel safe online. The next is being aware that the signs of abuse may not be obvious and can be physical, behavioural or attitudinal changes that are subtle and only come out when speaking with the person or when pointed out by someone else.

The most obvious sign is being shown or discovering an abusive social media post about your child that targets them directly.

	Your child is upset or unusually quiet every time they use the internet or social media.
	They are secretive about their digital activity, especially around social media or their phone.
	They are withdrawn from family or friends and spend most of their time alone in their room.
	Changes in their mood, behaviour, their sleep or eating patterns, especially after being online.
	They get nervous every time they get a message online or they refuse to discuss the content.

If you notice any of these signs, it may be worth asking if everything is alright at school, home or online.

Who are the offenders?

There is no profile for a cyber-criminal that can be used to fit every online crime. Each crime type brings its own profile and in some cases, the offender can be hiding in plain sight ranging from family members to co-workers to persons in positions of trust or authority. Online sexual offenders are often lone attackers seeking gratification from their victims, while those engaging in financially-motivated cybercrime are often more commercialised attackers where the criminal exploitation is managed as a business.

Members of an Organised Crime Group dedicated to this type of criminality operate in call centre environments contacting and seeking to exploit multiple victims at the same time to generate income and maximise the revenue they can generate.

Cyber hackers can typically range from a disgruntled ex-employee or competitor who has a score to settle to more organised international hacker group who are a motivated group that targets a company for commercial reasons such as ransomware demands or to extract potentially valuable data from their victim's computer network. They can also be state-sponsored hacker groups tasked with disabling a core infrastructure belonging to a rival country in what is effectively an online warfare attack. Attackers will seek to exploit a weakness in their victim or the system they are targeting. This can be a system that is running outdated software to someone who puts their personal data on a public social media account. Once the vulnerability is identified, they will deploy malicious software, enticing images or a phishing email which will hook their victim and give the attacker control, either of the system itself or the victim involved.

How can you help?

Regardless of your role or position, there are a number of ways you can support a child or adult who is a victim of social media abuse or exploitation.

EDUCATE YOURSELF

The first step is to be aware of the risks that exist when using online platforms. This comes from researching the risks and engaging with trusted online sources such as those listed at the end of this booklet.

This also includes ensuring that the social media platforms being used are appropriate and trusted, and that they have rules for both their use and for reporting when something goes wrong.

ENGAGE WITH VICTIMS AND POTENTIAL VICTIMS

The next step in the process is to create an atmosphere where your child, colleague, friend or staff are also aware of these risks and are comfortable reporting any concerns they may have. This is only achieved by openly discussing the risks and encouraging reporting in a non-judgemental atmosphere where the other person knows they will be helped and not punished.

SUPPORT VICTIMS

The next is that your response to someone telling you they were abused over social media is one of support, listening to what they want to say because it wasn't easy for them to take that step, offering safety, and encouraging them to share. This includes supporting them when they report it to Gardaí.step, offering safety, and encouraging them to share. This includes supporting them when they report it to Gardaí.

BELIEVE WHAT YOU ARE TOLD

However, the most important part of responding to any form of social media abuse or exploitation is believing the victim when they tell you what happened. Victims repeatedly say the worst part of what happened was not being believed when they finally told someone.

Who's influencing who?

The advent of the impacts of social media has seen a rise in the number of online influencers and personalities. These individuals use therir online presence to sell products or themselves, in return for payment and engagement by posting promotional videos or other materials online which are suggested as being essential for young viewers if they want to be successful.

With over 70% of children saying that digital creators are their heroes, it's clear their influence is high when it comes to choice of what to wear, what to buy and and even what to believe. However, some of those ideals can be unrealistic when kids see the perfect look or the best gadget as a must-have.

There is a new breed of influencer such as the 764 group or individuals who are goading children to commit crime, self-harm and even adopt radicalised beliefs that involve violence and abuse which is often gender or racist based.

This form of online exploitation often follows a set pattern where a recruiter who makes the initial contact with the child over social media with promises of friendship, reward or even threats if the child does not take part. The next stage sees an enabler taking over with the task of manipulating the child by sending them exploitative or violent videos in an effort to desensitise them and make them believe this is part of normal behaviour.

Once radicalised, the child is then convinced to commit acts of violence or other crimes in an ever-increasing cycle of threats, responses and rewards until it does become normal for them. Vigilance is key when it comes to personally identifying which influencers should be avoided and parents knowing which influencers are being viewed.

Rules for safe social media use

This brings us to the rules that every user should keep in mind when they log on to their social media profile, access their email account or start using the chat application they have installed on their mobile phone. These personal rules sit alongside the common sense rule of keeping private stuff private and differ from the rules imposed by the social media providers which govern who can use the platforms, the minimum age you can join at and similar parameters that aim to manage both users and use. Social media rules govern our online behaviour by setting out what we can and cannot do and could be compared to the manners that should accompany our online activity.

At its core, social media is a safe and secure communication tool as long as we follow the basic rules of ***Keeping it Locked, Keeping it Private, Keeping it Friendly and Keeping it Known.***

S	**SAFE:** Don't share personal information such as names, dates of birth, images or addresses online
M	**MEET:** Don't meet anyone you don't know on your own or unaccompanied. Let someone know.
A	**ACCEPT:** Don't accept emails, attachments, friends requests or messages from unsolicited sources.
R	**RELIABLE:** Don't accept everything you see online as fact or true. This includes profiles and offers.
T	**TELL:** Always tell someone about threats, abuse or mistakes you made, or online exploitation.

What preventions exist?

When it comes to online safety there are a number of preventions that can help to keep you and your children safe online. We have outlined above the rules that social media providers apply, the ones you should apply to your own activity and the ways that parents and guardians can help keep their children safe online. There are also general steps that can be taken to limit your exposure to online abuse over social media, and any other online platforms. Many of these are based on the maxim that if you wouldn't do it offline, don't do it online.

	Choose the right platforms for you or your kids - what will it be used for and are your kids safe?
	Protect your accounts and data with privacy settings and frequent updates from reliable sources. Don't respond to negative or abusive comments or content that you receive.
	Set your social media profiles to private and only post private content to friends that you know
	Limit the time you or a child spends online, especially at night.
	Know your digital footprint so you can delete any online accounts that you don't use or the fake ones with your name, image or contacts.
	Don't forget your mobile gives you access to all your online content but it is also a computer.
	Turn off location tracking unless you need it, e.g. for Google Maps - and use encrypted messaging.
	Same goes for Bluetooth and Wifi - they can identify you and your habits or connections.
	Set up Google Alerts for when someone searches for your name and personal information.
	Consider using activity-monitoring tools to manage and detect what your child is doing online.

What supports are available?

When it all goes wrong online, it is good to be able to reach out to any organisation or a friend that can help you understand what happened, support you during the recovery period because you are a victim, and help you get back online again safely. A number of online resources provide advice and support that can be used before and after an incident takes place - see below:

Hotline provides a mechanism for anyone to report websites and social media platforms offering, or being used to spread, illegal content, share private intimate images without consent, or other abusive activity. the website also links to other resources and provides information on a wide range of topics.

The **ISPCC Hub** is a useful resource on digital risks and abuses. It also offers advice to parents and teachers on how to respond when you or your child is a victim of abuse on social media or other platforms online.

An excellent resource for parents, teachers and young people on using the internet and social media safely. **Webwise** also provides downloadable resources for use at events and within your family groups.

An advocacy group for children, the **Cybersafe** page aims to inform children and adults about safely using the internet for schoolwork and personal activity.

The **Garda** website offers a wide range of advice and resources on crime in general, and specific advice and information on cybercrime, both dependant and enabled. It also outlines the reporting structures and paths available for victims of online and offline crime.

Social media takedowns

Any person who finds that offensive or abusive material has been posted about them online can ask the social media provider to take the content down using the platform's abuse link which can be found on almost every platform. Some of the most popular are listed below with links to their complaints page:

Meta provides one single link to report abuse and request a content takedown for all of its platforms.

Google provides one link to report abuse & request takedowns for its platforms like Google and YouTube.

X provides a platform for reporting abusive or illegal content and requesting a content takedown.

Tiktok also has a page for reporting abusive or illegal content and requesting a takedown. When requesting a content takedown, remember it's only a request and some providers may refuse.

Reporting online abuse or cyber crimes

Reporting online crime is very easy. Contact your local Garda Station. Where possible, bring along copies of any communications you received and sent, details of the online profiles, the advert you responded to, or the page that was used by the other person, and information about any payments you may have made, including the bank account or cryptocurrency wallet the money was paid to. For more information on staying safe online, please visit the **Garda website,** and safe online browsing.

An Garda Síochána