What would you do?

Brief for July 2017 theme for the localisation of the National Awareness Campaign 'What Would You Do?'

Digital and Online Abuse

The National Awareness Campaign as part of the Second National Strategy on Domestic, Sexual and Gender-based Violence 2016-2021

What is digital and online abuse?

In the last decade, technology has emerged as playing an increasingly significant role in how we build and maintain relationships with each other. The advent of the mobile phone, computers and the internet has revolutionised the ways in which we communicate. We now send each other texts, tweets, snapchats and selfies. Grandchildren in Australia can 'Skype' or 'Facetime' with their grandparents in Ireland and show them what they drew in school that day. Not too long ago such communication was the stuff of science fiction, now we take it for granted.

The options open to single people who wish to meet someone has also radically changed, first with the advent of internet dating and later with dating apps such as 'Tinder' and 'Grindr'. The role of technology in new relationships does not stop with introductions. Romantic partners frequently use digital means to connect with each other. The sending of intimate pictures has become so prevalent that, for many, it has seemingly become just another milestone in a relationship.

'Sexting', as it has become known can be part of a healthy relationship, a bit of fun between two consenting adults. However it can also have very negative consequences. A research study* into the 'Sexting' phenomenon found that while the practice was common among youths and young adults, 20% of participants reported being coerced into it at some stage. Furthermore these individuals were more likely to experience more traditional forms of intimate partner aggression such as physical, emotional or sexual abuse, suggesting that sexting coercion maybe an indicator of intimate partner violence.

Women's Aid, who run the national domestic violence helpline, are regularly coming across victims of domestic violence who report digital and online abuse as an element of the abuse they are suffering. According to their website** incidences of digital and online abuse reported to them includes:

- Women who are harassed and monitored online, through mobile phones and texting.
- Abusers who combine digital abuse with more traditional offline stalking tactics such as following, damaging property and abusive calls.
- Abusive partners who use the internet and social media to control and stalk women.
- Women who have personal details shared or lies spread about them and are impersonated by their abuser online.
- A common form of digital abuse reported are damaging rumours being spread about women both personally and professionally and having sexually explicit images and videos that were taken with consent posted online without consent ('revenge porn').
- Abusers have advertised their partners on escort sites without their consent or knowledge.
- Abusers have used specific spyware to monitor the woman, find out her online and bank account passwords and keep track of her whereabouts.

* (Drouin et al, 2015) 'Sexting: A new digital vehicle for intimate partner aggression'
** https://www.womensaid.ie/help/digitalabuse.html

What is digital and online abuse?

The incidents of digital and online abuse that are being reported to Women's Aid, indicate that the use of technology in a relationship can often take a sinister turn when couples breakup. Where in the past couples contested ownership of property, pets or CD's, now many are faced with the issue of what happens to intimate pictures or recordings that were taken in happier, more trusting times. Unfortunately, there have been documented cases where people's lives have been turned upside down, or even driven to suicide, by ex-partners taking those intimate images and posting them online. Such incidences have become known as 'Revenge Porn', named after online 'ex- girlfriend' pornography sites that began to specialise and market such material.

There have been reports in the media of cases such as 'Niamh'* (name changed) who after splitting up with her boyfriend, logged onto Facebook to find that someone had accessed her account and changed her profile picture with a naked picture of herself. Even more disturbing was the fact she had no recollection of the photo being taken and she appeared to be asleep in the photo. When her ex-boyfriend commented on the photo, she knew it was him. Last year the 'Sean O'Rourke Show'** featured a guest who discovered that four years after breaking up with her boyfriend, he had posted online a sexually explicit video of the two of them, again recorded without her knowledge or consent.

Often in the discussion around revenge porn, much like the stealing of intimate images in the infamous 2014 celebrity hacking scandal, commentators blame the victim for taking the pictures in the first place, rather than vilifying the person who shares it with others. According to statistics from the Cyber Civil Rights Initiative, 47% of revenge porn victims contemplate suicide***.

*The Irish Independent, 15/7/2014
** RTE Radio 1, 21/6/2016
*** https://www.cybercivilrights.org/

Digital and online abuse and the law

The emergence of digital and online abusive situations has created new challenges to law makers and police agencies, both in Ireland and internationally. Currently, digital and online abuse cases fall under Section 10 of the Non-Fatal Offences against the Person Act 1997. This section has been used to successfully prosecute individuals who committed harm via communications through messaging/online in the following cases:

- A man was convicted of harassment and given a six month prison sentence for creating a fictitious social media account using photographs of someone he knew. He also included photographs of similar looking women from pornographic sites and contacted over 1000 men posing as the victim.
- A man was convicted of harassment after he posted a video of him and his former partner engaging in sexual activity to a pornographic website. When Gardaí contacted the site to have the video removed, he posted the video to the same site again. The victim was unaware that he had even recorded the video in the first place. This was reported in the media as 'revenge porn' despite there not being a specific offence to cover revenge porn in Ireland to date.
- A woman charged with harassment for sending hundreds of unwanted text messages and WhatsApp messages to a man with whom she had two dates. Some of the messages were graphic. She was ordered to stay away from the victim and not to contact him by any means.

As can be seen, there have been some successful prosecutions for harmful communications using the current legislation. However, a recent report of the Law Reform Commission (LRC) on Harmful Communications and Digital Safety (2016) has highlighted areas where the law could be strengthened and where new offences may be necessary. Following Government approval drafting of a general scheme of a Bill is currently underway in the Department of Justice and Equality. It is intended that this legislation will provide for the following recommendations of the LRC:

- The strengthening of the offence of Harassment under Section 10 of the Non-Fatal Offences against the Person Act 1997.
- The creation of a new offence of stalking.
- The creation of two new offences relating to the distribution of intimate images without consent.
- The replacement of the existing offence of sending grossly offensive, indecent, obscene or menacing (or in some cases false) messages which is contained in section 13 of the Post Office (Amendment) Act 1951.

The LRC report also proposed the establishment of a Digital Safety Commissioner to promote digital safety, to publish a statutory Code of Practice on it and to oversee efficient take-down procedures to ensure that harmful communications can be removed as quickly as possible from social media sites. The Department of Communications, Climate Action and Environment are currently considering these recommendations.

How to protect yourself from digital and online abuse

In recent times, groups such as Women's Aid and The National Network to End Domestic Violence (NNEDV) have created excellent guides on how victims of domestic abuse can protect themselves from digital and online abuse. The following information is specific to victims of domestic and sexual violence and has been adapted from a Women's Aid (UK) publication titled '*Digital Stalking: a guide to technology risks for victims'* *.

<u>If you are planning on leaving an abusive relationship</u>

- **Don't use your home computer**. Stalking behaviour often starts before a victim leaves their home. All victims should assume that their computer is being monitored.
- **Do not use your computer** or existing e-mail accounts to make plans or inform anyone that you are planning to leave. Use a safe computer (one that the perpetrator could not have installed software on or that they monitor) such as a friend's or a library computer.
- **Create a new e-mail account**. Use a safe computer to set-up a brand new e-mail account. Don't access the new e-mail account on your old computer – remember the abuser may be monitoring it. Don't use password or security answers the abuser could guess. Only use this e-mail account to contact those helping you to make plans.
- **Don't use your smartphone**. When you leave, disable your smartphone so you cannot be traced. If you have an Android phone turn it off and remove the battery. If you have an Iphone then all you need to do is turn it off to stop transmission of your data. Buy a cheap mobile phone. You can get them for €10 at a supermarket.
- **Check your car**. If you plan on leaving in your car, check for a GPS tracking device. Consider using a taxi/bus or meet a friend in the next road. If you continue to use your car, the abuser may try to find the car and you.

<u>Once safe and away from the abusive relationship</u>

- **Change passwords.** As soon as possible, use a safe computer to change the password on your existing e-mail account(s) and mobile accounts e.g. Google, iCloud. At the same time, change any secondary contact e-mail address to your new account(s). Remember to change your social network accounts, online banking, eBay, PayPal, online stores etc. Call your mobile phone company and change the security PIN/passwords.
- **E-mail accounts**. It is better to use multiple e-mail accounts. It means that if the perpetrator gets hold of one of them, you have an indication of where there is a security issue. It also means if they get hold of one e-mail account the others are still safe to use. If you use a service like Google mail you can manage them all easily. Create separate e-mail accounts for: most trusted friends and family; social networking – other friends; online registrations; financial account.

*https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

How to protect yourself from digital and online abuse

- **Making your computer safe**. If you want to start using your own computer again, then you need to buy anti-spyware software and run a full scan. If you don't have antivirus software on your PC then you should also install one of these products and run a full scan.

Securing mobile phones

- **Use secure login/passwords.** Change your login/password to your online account. Choose a password that the perpetrator will not be able to guess.
- **Always use a PIN.** Activate your phone security settings so that after a minute of non-use, you have to put in a PIN before you can use the phone. Choose your PIN carefully; don't use your birthday, anniversary, child's birthday, 0123 or 9876 – they should be random numbers.
- **Mobile security software.** Invest in mobile security software. It will prevent spam and virus software on your mobile. Most of them provide call blocking using whitelists. If you suspect that the perpetrator had access and could have put spyware on the mobile then you need to buy software to remove it.
- **Call blocking**. Either use the call blocking features in your mobile security software or buy an online app that offers call blocking using 'whitelists'. Call blocking using whitelists means that you can only be contacted by someone in your address book and all other calls will be blocked. There are options of what you can do with the blocked number such as send it directly to voicemail or hang-up. Make sure you delete all contact numbers you have for your abuser and any other of their friends and family numbers that they may use to contact you.
- **Apps.** Delete all apps that tell you where you are: maps, photos, check in, find my phone etc. You can reinstall the apps you want again later. When installing apps pay close attention to what you are allowing them to do. If the app asks for administrator access, say no.
- **Understanding geolocation.** Learn how to turn on and off your wi-fi, GPS and geolocation services, and change the default so that geotags are not added to photos.

Using Social Media

- **Block the perpetrator**. Even if they are not on your friends list. Also, block all their friends and family.
- **Be careful of adding any new friends**. Perpetrators will often create fake e-mails and profiles of friends and family so you will add them to your friends list. Before you add a friend or family member, just call or e-mail them to check they really sent you a friend invite. If the perpetrator does use a fake profile block it immediately and inform friends and family on your friends list, asking them to block it as well.

How to protect yourself from digital and online abuse

- **Reduce your friends list**. The more friends you have on your social network the easier it is for your abuser to find out information about you.
- **Change your privacy settings and your security settings**. This will vary depending on what website you are using.
- **Use login notification feature**. Make sure your perpetrator is not accessing your social network by logging in and pretending to be you. Change your security settings to get notifications when a new device tries to login to your account.
- **Tell your family and friends**. Stalkers not only stalk you, they will also contact and follow your friends and family via social networks. Let friends know that the perpetrator may try to: contact them; send a friend request; create fake profiles to send friend requests; chat with them to try to find out more about you, or spread lies about you. Ask friends to**:** block the abuser and their friends and family – if they won't do this, then you will need to remove them from your friends list; make sure that they have their privacy settings on friends only; not to post any contact details for you or respond to anyone who asks for them; not to post pictures of you or tag you in any photos (if they do, then remove the tags); let you know if the abuser contacts them or if they are using a fake profile.

<u>Removing Material from Social Media Sites</u>

Under current non-statutory, self-regulated arrangements, individuals can report harmful content to social media sites and request that it be removed. All the prominent social media companies have content and conduct policies and standards, which outline their approaches to different categories of harmful content, including hate speech, sexual violence and exploitation, serious threats, harassment and related activity, creating fake profiles, posting private information without consent and content that would promote self-harm. Not all of these categories appear to be treated in the same way, with removal more likely in the case of some types of content rather than others.

What help is available?

Although new protections for victims of digital and online abuse are currently being drafted into legislation, as earlier outlined there are already laws in place, which make many aspects of digital and online abuse a crime. It is important that where there is a suspicion a crime has taken place a report is made to the Gardaí.

The 'What would you do?' campaign website has a dedicated section on digital and online safety. It has information on how to wipe your internet history, as well as information on how to cover your tracks when browsing the internet going forward.
See http://whatwouldyoudo.ie/#page-safety

Women's Aid is the leading organisation in Ireland dealing with domestic violence in Ireland. As well as providing services to women who suffer abuse at the hands of their intimate partners, including a 24hr helpline, their website has an extensive area concerned with digital and online safety. Some of the areas covered include information on types of digital and online abuse, how you cover your tracks online, how to check for spyware and details on how to protect yourself on social media sites. There are also publications, both Irish and international, available to download on their website, including a recently published collaboration with Facebook on how victims of domestic abuse can stay safe on the social media platform.
See https://www.womensaid.ie/help/digitalabuse.html

The National Network to End Domestic Violence (NNEDV) is an American organisation that has published extensively on how victims of domestic violence can protect themselves from digital and online abuse. They have established the 'Tech Safety' project which, as well as providing regularly updated information for victims of digital and online domestic abuse, also provides information for professionals who work with victims of domestic and sexual violence.
See http://nnedv.org/internetsafety.html and https://www.techsafety.org/

Paladin is the UK national stalking advocacy service. As cyber stalking is increasingly becoming a feature of domestic abuse, they are also a great source of information on how victims of domestic abuse can learn to protect themselves online and in the digital world.
See http://paladinservice.co.uk/advice-for-victims/

Advice for bystanders/witnesses concerned for someone they know

Don't wait for them to approach you. Look for a private moment where you can express concern and let them know you're there to support them. A simple question like "are you ok?" could give you both an opportunity to talk.

Express concern

Tell your friend that you've been concerned for them or that you're worried. This is a non-judgmental approach that might make them feel comfortable in opening up. If they deny that anything is wrong, don't push, but communicate that you'll be there for them if they ever want to talk.

Assure them that the abuse is not their fault.

This can be such an important thing for a victim of abuse to hear. Some useful things to say might be, "No one deserves to be treated this way," "You are not to blame," or simply, "What's happening is not your fault."

Support, but don't give advice

This can be so hard to do, especially if the victim is someone close to you. But remember that you cannot make someone leave a relationship if they are not ready to do so. **Be aware that leaving an abusive relationship is the most dangerous time for a victim. The victim is best placed to assess the danger to themselves.** Give them options and offer to help and support them along the way, but pressuring a victim to leave a relationship who does not want to may only isolate them further by making them feel they can't confide in you. Remember that abusive behaviour is a pattern of getting power and control over someone else. Validating a victim's choices and encouraging them to make their own decisions about their life can help to break the cycle of power and control.

Give resources

There are plenty of services in Ireland which can offer help and support to the person you are concerned about. Check out www.whatwouldyoudo.ie for a list of services and advice on how to find the most appropriate one.