
ORBITS
Taxonomy of tech abuse

Taxonomy of tech abuse

This section includes a non-exhaustive list of common forms of tech abuse that we refer to throughout this field guide.

Creep shots (upskirting/ downblousing)

Creepshots refer to the use of mobile phones and cameras to take 'up the skirt' or 'down the blouse' images of someone without their consent. Such images are generally taken of unwary users of public transport, restrooms, and elevators and are sometimes also circulated or published online. In the UK, police receive upskirting reports from at least one survivor every day, including many children.

Cyberflashing

Cyberflashing is the sending of unsolicited sexually explicit images or videos, without the receiver's consent. It is also commonly known as 'sending unsolicited d*ck pics'.

This can be experienced as a one off event or part of ongoing abuse and harassment. It can also include one or multiple images and/or videos. While cyberflashing can be perpetrated by someone known to the victim via social media accounts, dating apps and messaging platforms, it can also be done in public and by strangers using Bluetooth and AirDrop technologies. Many international studies found that around 50% of young women aged 18-25 have received penis images without consent, with prevalence increasing for girls under 18. A 2020 University College London survey of 150 young people aged 12-18 in the UK revealed that 76% of girls under 18 have been sent unsolicited sexual images on social media.

Cyber harassment/online harassment

Cyber harassment is the repeated harassment or threatening of an individual(s) in digital spaces. This often includes persistent unwanted communication and hateful comments. It might also include making threats of further offline abuse, such as physical or sexual violence.

While anyone can experience cyber harassment, those with multiple

marginalised identities are targeted disproportionately, and the problem is particularly acute for women in the public sphere, such as politicians, journalists, and activists. For example, in the USA, female legislators are 3.5 times more likely than male legislators to receive threats of bodily harm on Twitter, and politicians who are women of colour are twice as likely to receive tweets about their gender or body as their white women counterparts. Pollicy carried out a study into online violence during the 2021 Ugandan general elections, and found that women candidates were more likely to experience trolling (50% vs. 41%), sexual violence (18% vs. 8%), and body shaming (14% vs. 11%) in comparison to their male counterparts.

Research by Amnesty International on India's 2019 election found that one in every seven tweets sent to women candidates were abusive or problematic, and Muslim women received 55% more abuse than others. In the UK, Amnesty International carried out research into the online harassment of women members of parliament (MPs) active on Twitter in the run up to the 2017 general elections and found that 20 racialised female MPs received 41% of the abusive tweets, despite there being almost eight times as many white women in the research. The UK's first Black female MP Diane Abbott received nearly a third (32%) of the overall abuse.

Cyber stalking

Cyber stalking involves the monitoring of an individual's location and activities through geo-location trackers or monitoring their use of the internet. This might involve closely following their social media activity to find out where they are - for example if they post a photo in a recognisable place, geo-tag an upload with a location, or 'check-in' to a venue. It can also involve employing stalkerware to track someone's movements and actions. Intimate partners, as well as strangers, resort to cyber stalking, and it is often part of a larger pattern of controlling and coercive behaviour, including offline stalking. Cyber stalking can also involve using wearables and tracking devices, such as AirTags.

Digital morphing/Deepfakes

Digital morphing is the use of technology like Photoshop or AI to create a photograph or video, in which a person's face is morphed or superimposed on the image of another person's body. Perpetrators use, or pay another individual to use, such

morphing technology to create fake nudes, explicit images, or videos. These are often used to perpetrate further forms of image-based abuse as outlined below. A 2018 analysis of 7,964 videos, by Amsterdam-based cybersecurity company Sensity (formerly Deeptrace), found that 90% of deepfake content online involves non-consensual deepfake pornography, where women's faces are superimposed onto naked or sexual images.

Out of the top 10 pornographic websites that host deepfakes, nine websites are monetised entirely by them. An investigation into a version of the app DeepNude on the messaging app Telegram revealed that over 680,000 women had their images stolen from their social media accounts or private conversations, which were then manipulated and sexualised. Terrifyingly, the number of deepfakes on the internet is thought to double every six months.

Doxxing

Doxxing is when perpetrators purposefully leak previously private and personal information online. By publishing details like name, contact number, email address, and home and office address publicly, victims are exposed to unwanted attention and possible harassment, threatening their safety and mental health. A 2021 study by SafeHome found that 21% of Americans, over 43 million people, had experienced doxxing.

Gendered disinformation and gender trolling

Gender trolling is when gender-based insults or hate speech are shared online. Similarly, gendered disinformation involves the spreading of false or misleading gender-based narratives, often with some degree of coordination. Common false narratives include those manipulating gender stereotypes about women, lying about gender equality, and fabricating information and statistics about contentious issues related to gender. In all cases, the sharing of such speech is often coordinated by groups, meaning survivors experience a barrage of such messages. This form of abuse is often intended to deter women from participating in public life.

Image-based abuse

Image-based abuse includes all forms of non-consensual taking, creating, altering, or sharing of (including threats to share) intimate images or videos. While this is generally understood as

referring to sexual or nude images, we define 'intimate images' as any image which shows someone as they would not normally be seen in public. For example, for someone who usually wears a headscarf or other form of religious garb, a photograph of them without it would constitute an intimate image. Image-based abuse is often referred to as 'revenge porn', but this term is generally rejected as such material should not be viewed as porn nor revenge and the term obscures the complexity of the issue.

There are often multiple, overlapping motivations for image-based abuse, including harassment, humiliation, and public shaming, status-building among groups of men, sexual gratification, and sometimes financial gain. The perpetrator may leverage image-based abuse to get a survivor to stay in the abusive relationship, for sexual favours, for money, or to scare or silence them from disclosing abuse. Threatening to share intimate images is image-based abuse, regardless of whether the images are actually shared or not.

Sex workers are particularly at risk of image-based abuse, as their content is often distributed without their consent. A study by LegalJobs in 2021 found that pornography is one of the most pirated materials on the web, with an estimated 35.8% of pornographic material being pirated online. Similarly, a recent investigation discovered "an entire supply chain of people stealing sex workers' labour using scraping programs without permission, in some cases by the hundreds of terabytes, and distributing it on other adult sites or selling scraping services through Discord."

Refuge, a UK based organisation that works with victims of domestic violence, conducted a survey of 2,060 people in 2020, and found that 1 in 14 women had been threatened with image-based abuse. For young women aged 18-34, this number rises to 1 in 7.

Impersonation

Impersonation is when a perpetrator uses technology to pretend to be someone else. Typically, a perpetrator creates fake social media accounts using the name and image of the person they are impersonating. They may use these accounts to share content or send messages that are harmful to the person in question, such as sending obscene or offensive messages to their personal or professional contacts.

Outing gender identity or sexuality

The outing of a person's gender identity or sexuality may be done on online platforms, either publicly or to their family and friends without that person's consent. This kind of abuse targets LGBTQ+ people who may not have disclosed their gender or sexual identity to everyone or certain people.

The caller may pretend that the call is a misdial or will hang up every time the call is answered. This form of harassment is particularly common in lower-income, rural communities, for example in India.

Repeated wrong dials

Repeated wrong dials refers to the instance where someone is regularly 'miscalled' by another individual, often from an unknown number.

Smart-home abuse/domestic digital abuse

Smart-home abuse is when a perpetrator manipulates technology or Internet of Things (IoT) devices that control someone's home environment, for example light, sound, temperature, or locks. This kind of abuse is usually seen in the context of domestic abuse as part of coercive control. An abuser might make the home excessively hot or cold, might switch lights on or off, or play music or noises to impact their partner's physical and mental wellbeing. Devices used for smart-home abuse include ring doorbells, Amazon Alexa and Echo, Google Home Hub, CCTV cameras, and more. Often this abuse is carried out via smartphone apps, even if the abuser is far from home. Smart-home abuse can also involve intrusive tracking through digital devices, such as watching someone's movements through sensors or security cameras, or eavesdropping through microphone-enabled smart devices.

Zoom bombing and Zoom flashing

Zoom bombing takes place when individuals disrupt online video calls without authorisation and inundate participants with unsolicited and disturbing content, such as graphic sexual images, videos or/and derogatory words. Zoom flashing is when someone exposes their genitals live online after infiltrating an online meeting. These activities have increased during the pandemic, when most work and education shifted to online platforms. Named Zoom bombing because of the popular video-conference tool Zoom, it can happen on any video-calling software including Skype, Microsoft Teams, and Google Meet.

While Orbits focuses on TGBV, there are other forms of online or technology-facilitated harm which impact women and people of marginalised genders.

For example, many young men are being groomed into misogynistic attitudes online, which in turn produces perpetrators of TGBV (and other forms of GBV).There are other forms of online abuse and harm that are beyond the scope of this guide, including identity theft, use of opaque algorithms, online scams, and online child exploitation. For an overview of different categories of online harm, see the Online Harassment Field Manual.

The impact of tech abuse on survivors

> *"Some victims had to move from the town they live in. Some people, like the founder of our organisation, have had to change their names. Some have died by suicide."*
>
> Mary Anne Franks, Miami School of Law

Like all forms of GBV, tech abuse can be devastating for those who experience it. While the impact on each survivor is different - it may be influenced by a range of factors including the nature of the abuse, where the survivor is based, their personal life circumstances, and different aspects of their identity - there are several common themes for the way tech abuse affects survivors.

Physical safety

Online violence often endangers and impacts a survivor's offline physical safety. In some cases, this form of abuse can be carried out by perpetrators who first identify the survivor through some form of tech abuse and then continue to stalk, harass or threaten them. In some cases, survivors' physical safety may be threatened by family members or other close contacts, who carry out violence as a disciplining or punishing act.

Mental health

The impact on survivors' mental health can be deep and serious. Instances of post-traumatic stress disorder (PTSD), paranoia, anxiety, and depression are recorded frequently. Many survivors report severe trust issues and self-image problems as a result of tech abuse. For many, the impact is long-term as they do not regain the confidence or sense of safety they had before the abuse. They may restrict their use of technology, or withdraw from online spaces completely. The helplessness that ensues when one is unable to control their information on the internet gives rise to prolonged trauma that often manifests in unpredictable ways. Some may have suicidal thoughts or move towards a more reclusive life. The lack of help or support pushes many to find their own coping mechanisms, which can lead to further issues like drug abuse, alcoholism or self harm. 35% of survivors report mental health issues as a result of experiencing online violence, and 43% feel unsafe.

Relationships

Due to stigma and prejudice against them, survivors often experience a severe negative impact on their relationships. Given that many forms of tech abuse involve a public element (for example, sharing intimate images publicly or with a survivor's friends/family/acquaintances), this a particularly pertinent concern. Even if the abuse does not involve a public component, survivors often face this impact if and when they decide to disclose their trauma to those around them. Some survivors are completely ostracised by family members and/or social and professional circles.

Often, they experience victim blaming, where they are blamed for the violence inflicted upon them. 23% of survivors said that their experience of tech abuse had caused harm to a personal relationship. The negative impact on relationships can create feelings of loneliness and isolation, which in turn often contributes to further mental health consequences.

Reputation

Often, perpetrators of tech abuse use survivors' reputation as leverage to inflict harm. A survivor may suppress the instance of abuse or continue to maintain a relationship with the perpetrator in an attempt to preserve their reputation. But when tech abuse is disclosed, whether by the perpetrator or the survivor, the social backlash can be extensive. Survivors have lost jobs, been expelled from school, college, or university, had to change their identities, and even relocated to different cities. Often survivors feel they have to completely change their lives to create a new image and reputation and leave behind the so-called 'tarnished' one.

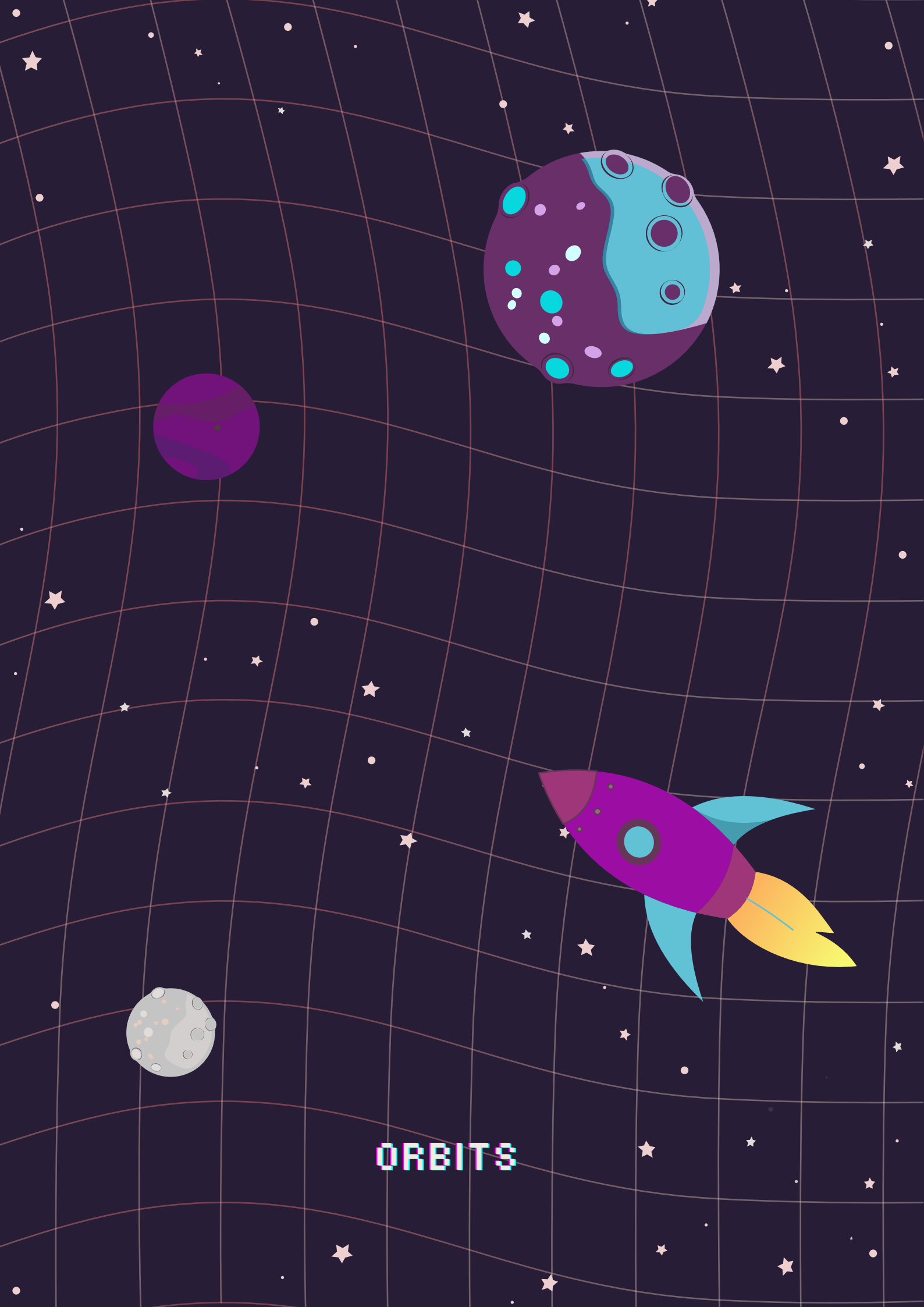
Economic

There are often serious economic impacts for survivors of tech abuse. The experience itself can create multiple costs (legal fees, therapy costs, replacing compromised devices), whilst the reputational impact can create further costs (the cost of relocation or losing your job) and impair a survivor's ability to generate income by impacting their employment prospects.

Self-censorship

Tech abuse can inhibit a survivor's freedom of expression as they may self-censor, or remove themselves from the online sphere completely due to shame and fear of further abuse 58% of those surveyed in a global survey titled 'Free to be online?', conducted by Plan International with 14,000 women respondents from 22 countries, have experienced online harassment on platforms such as Facebook, Instagram, Twitter, WhatsApp, and TikTok. 19% of these girls reported leaving or reducing usage of specific social media platforms after being harassed, while 12% stated that they changed their behaviour on digital spaces to avoid harassment.

Tech abuse can even have a silencing effect on those who have not experienced it directly. Knowing about the existence and prevalence of tech abuse can sometimes be enough to discourage people from having a presence on social media and/or taking up public positions. This in turn entrenches gender inequality, by providing additional barriers to women taking up positions of power and/or expressing themselves. Nearly 9 in 10 women restrict their online activity, and 1 in 3 think twice before posting any content online.


ORBITS