DART CENTRE ASIA PACIFIC
A PROJECT OF COLUMBIA JOURNALISM SCHOOL

Five tips for protecting yourself against
Technology-Facilitated Gender-Based Violence (TFGBV)

In recent years, we've seen an exponential increase in attacks on women and minority journalists in the course of their work, where harassment and online violence are used to silence voices.

With each journalist silenced, we lose a valuable voice and the diversity of perspectives in the news that we consume is diminished.

Nearly three-quarters of 1,210 women journalists surveyed in 2020 said they had experienced online abuse, harassment, threats and attacks, with 20 per cent of the women surveyed reporting offline abuse and attacks they believed were seeded by technology-facilitated gender-based violence (TFGBV).[1]

These five tips for protecting yourself against TFGBV are informed by evidence, expertise from Dart Centre Asia Pacific (DCAP), and the lived experience of journalists who completed the inaugural TFGBV Fellowship offered by DCAP with funding support from Google News Initiative (GNI).

Fellows have generously translated this tip sheet into multiple languages, including Hindi, Filipino, Fijian and Chinese. Tip sheets in these languages are available to download from the Dart Centre Asia Pacific website: https://dartcenter.org/asia-pacific

1. Be social-media savvy

- Understand the digital platforms you are working on, including the key online threats common in these online spaces
- Attend a social media self-defence webinar and learn how to recognise online abuse and its impact on women. The Australian e-Safety Commission offers a range of free webinars that can help you set up your social media accounts and profiles with safety in mind. Its webinars also cover how to deal with online abuse through muting, blocking and reporting (https://www.esafety.gov.au/)
- Know the laws in your country that address TFGBV as well as the safety of journalists. Understand how that legislation is being implemented
- Understand where you are most vulnerable (e.g., Facebook, X, LinkedIn, Instagram).

2. Bolster your cybersecurity

- Use long passwords (ideally a string of words and symbols), never re-use passwords, create answers to security questions, and set up two-factor authentication on your key personal and professional accounts (e.g., email, social media, banking)
- Try to keep your personal and professional profiles separate
- Limit the amount of personal information you share on public profiles (e.g., avoid showing pictures of your children, identifiable landmarks, pets, etc)
- Do not use your work email address for private profiles
- Do not use the same profile image for both professional and personal accounts
- Do not re-use handles across platforms that you'd like to keep separate
- Talk to your friends about tagging! (You may not want them to tag your personal accounts when sharing your professional work, for example)
- To protect your privacy, it is recommended to use a VPN
- To prevent doxxing, search your name on Google to see what information shows up about you (e.g., your address, your phone number, other private/personal information which would make you contactable). It would also be wise to search just your phone number, or other personal information to see if anything comes up there too. If you discover that your personal information is available to the public, you can request Google to remove that information from search results using this form: https://reportcontent.google.com/forms/rtbf

- Have a clear idea of the level of personal information, including images and videos, that is available on your profiles.

3. Document and report TFGBV

- Be sure to document any instances of TFGBV. If you report online abuse and succeed in getting it taken down, you could lose valuable evidence. Save emails, voicemails and texts. Take screenshots on social media and copy direct links whenever possible
- Ensure the documentation is saved in secure, multiple formats
- Assess and monitor the origin, characteristics and frequency of the threat. Consider carefully whether the threat might transition offline. You can assess this based on the type of harassment. For example, if the perpetrator is known – or if they show any sign of stalking or revealing personal information about you that you didn't previously publish online (such as a home address, car plate number, pictures of private reunions, etc.) – the threat is probably real and it is recommended that you report it. If you believe that the threat is intended to be exclusively online, you can report the user to the platform you are using, or use the block feature
- If experienced repeatedly, create a log that can help identify patterns and establish an evidence base for a claim of TFGBV
- Block, mute and report abuse on social media platforms
- Assess your safety. Is the threat directed and specific? Does it include your name, a time, a place or a method of attack? Does the abuser seem irrational, for example, threatening you using their real name, email or phone number? Has the abuser migrated across platforms or moved offline (e.g., voicemails, physical mail or packages left at your door or workplace)? If you're being made to feel unsafe in any way, report it to your manager.

4. Know when to engage

- The standard advice "Don't feed the trolls" is often sound. When confronted, abusers may escalate attacks or try to provoke their targets into lashing out to get them in trouble. Speaking out against abuse, however, can also be profoundly empowering
- The key is to be careful and deliberate as you decide what will work for you. One way to do this is to practise counter-speech without directly confronting your abuser. Counter-speech could involve forcefully denouncing harassment and hate, defending your reputation and fact-checking disinformation
- Understanding the context of the abuse is also important. Would you engage if you knew the abuse was coming from a bot instead of a human?

5. Build a trauma-informed community of support

- Discussing TFGBV can elicit feelings of fear and shame, so it is important to remember that abuse is intended to isolate you. Remember: YOU ARE NOT ALONE
- Seek support from friends, family, colleagues, professionals and deploy your wider cyber community to serve as allies
- Support your colleagues. Having conversations and sharing lived experience of TFGBV can help break down the stigma associated with seeking help. Talking things through with colleagues can help see a different perspective.
- Enlisting allies can help: Trusted friends or colleagues can keep tabs on your mentions while you're blocking and muting.

1. Posetti, J., & Shabbir, N. (2022). The chilling: A global study of online violence against women journalists.