Freelancer Online Violence and Abuse Handbook

Why it is important to prepare for online violence and abuse:

Online violence and abuse doesn't seem likely until it actually happens to you. It can affect your day to day life, your physical safety and mental wellness.

Online violence and abuse can be harassment in the forms of sexual harassment, hate speech, doxxing (*publishing of personal data online such as your address & phone number*), threats against family members, threats of sexual violence, death threats, just to name a few.

These forms of harassment can be done through platforms such as email, SMS, Messaging apps, such as iMessage, Twitter, Facebook, Instagram, Tik Tok, etc.

Things to keep in mind when it comes to online violence are: how publicly available is your information such as your social media, your number, address, places you visit and can people like family and friends be connected back to you. Are your social media accounts secured (read more below) and **note that you are more vulnerable to experiencing online violence after a story with your byline is published, whether you did reporting or visuals.**

Examples of online abuse at *Cicero Independiente*

We as *Cicero Independiente*, published an article, [Cicero Police Employee Accused of Domestic Violence Kept Job Despite Investigator's Warning](#), once published we received anonymous emails using foul language. In addition, after this article, the co-founders of Cicero Independiente received an odd letter with a story tip to their home addresses.

Furthermore, when *Cicero Independiente* hosted a candidates forum in 2020, people used one of the co-founder's organizing background to make claims that she was not an objective reporter and attempts were made by local residents and local officials to discredit *Cicero Independiente*'s election coverage. It is a common tactic by politically connected individuals in both two local municipalities to look through social media of a potential target and use past posts to mischaracterize them.

Freelancer Online Violence and Abuse Handbook

Cicero Independiente has since put together some resources to better protect you should you experience online violence.

In preparation:

A suggestion is to google yourself and see what information is available on you and your loved ones in connection with your personal information.

The following information has been amended from the International Women's Media Foundations' Guide to Protecting Newsroom's and Journalist's Against Online Violence.

Look yourself up online using all search engines
- Use incognito mode or a private window function to carry out the search. You can find this by clicking the three dots in the top right of your browser.
- Use Boolean search terms to get a more in-depth look at what is out there on the internet about you.
- Review images and video on search engines searches as well as looking at comments under news you may have written.
- Right click on a photo of yourself to carry out a Google image search. This will show you on what other sites that image appears.
- Review your social media and look through photos, comments and old posts
  - Do you have location tags on a public profile (anyone can access this information)
  - Are places you visit highly recognizable
  - Are there photos, comments or old posts that you or others you wouldn't want to be downloaded or screenshotted
- Note down any data you would like to remove
- [Dox yourself](#)

Remove data from the internet
- Remove or make private content on your social media accounts
- Check the privacy settings of your social media accounts and also help family members to do the same. If an online abuser can't find information on you then they may try to find content on the sites of your family.
- Remove personal content from sites that you own, such as a personal website

These online harassment policies and procedures were created with support from the International Women's Media Foundation.

Freelancer Online Violence and Abuse Handbook

- Ask family, friends, colleagues to remove their content with your information from sites or social media accounts
- Check internet archive services, such as the [Wayback Machine](), and ask them to remove content
- Consider requesting Google Maps/Apple Maps to blur out your house
- Ask Google Search to remove unwanted data from its search engine
- Contact owners of websites or public databases to see if they will/are able to remove data about you
- **Cicero Independiente can provide you access to a data removal service, *[DeleteMe]()*, *for a year*, to scrub your personal information and data from different broker sites.**
  - Freelancers that qualify are those who currently have a byline on 3 or more stories in the current calendar year. This includes reporting and visual freelancers.

How to protect your personal accounts:

Secure your accounts
- Turn on two-factor authentication (2FA) for all your accounts. Use an **authentication application,** such as [Authy](), for this.
- Consider using a [password manager]() and create long passwords of more than 16 characters.
  - The longer your password is the more secure it is
  - Use a mixture of numbers, symbols and letters OR use a collection of words that have no connection to each other, for example, *signpostgiraffeswimmingpool*
  - Do not store your passwords in your browser
  - Use a different password for each account.
  - Do not include personal information, such as your date of birth, in your password. This is information that is easily found about you online.
- Backup Codes provided by social media managers (ex: Instagram)
- Use the following best practice for Twitter:
  - Turn on 2FA
  - Be mindful about what personal data you may have public facing
  - Turn on protect my tweets
  - Change photo tagging and who can tag you
  - Turn off location settings
  - Check how your account is discoverable, by email or phone number and how easily accessible those are
- Use the following best practice for Facebook

CICERO INDEPENDIENTE

Freelancer Online Violence and Abuse Handbook

- ○ Who can send me a message or friend request
- ○ Who can look you up by email or phone number
- Learn more about securing your accounts **here**

Other
- Set up Google Alerts for your name, address and date of birth
- Create calendar reminders to review your online profile regularly

What to do if you begin experiencing online violence of any form:

- Document the harassment, take screenshots of messages, comments on your personal social media or record videos if you are being verbally harassed in person or followed, just to name a few examples.
- Let [main contact] know of these occurrences: [email address]
  - ○ In a meeting we will go over with you what needs you have that are to be met to secure your safety.
    - ■ Do a risk assessment with you to plan alternative routes home, a safe word and who to contact if you are in immediate danger and need someone to come get you, and other ways to contact your loved ones.
    - ■ Rather than provide a source with your personal phone number, provide them a google voice number to contact you with
  - ○ Resources: Cicero Independiente has a fund for immediate assistance
    - ■ Housing Cicero Independiente can provide:
      - ● Airbnb/hotel coverage for 1 week
    - ■ Legal
      - ● Reporters Committee For Freedom of Press legal hotline and resources
      - ● Media Defense
      - ● LNJAR Media Help
      - ● Chicago's Lawyers Committee for Civil Rights - get legal advice from volunteer attorneys
    - ■ Mental Health Services

IWMF INTERNATIONAL WOMEN'S MEDIA FOUNDATION

Freelancer Online Violence and Abuse Handbook

- - Cicero Family Services
  - National Alliance on Mental Health
  - Suicide Prevention Hotline
  - Organizations:
    - Sarah's Inn, a nonprofit organization that may be able to provide assistance creating a safety plan and provide housing
    - Domestic Violence Legal Clinic at Ascend Justice helps with orders of protection
- If your account is hacked, notify [main contact] and we will go over
  - Two factor authentication to gain back your account
  - Change your password
    - Password length matters more than random characters
    - Passphrase instead of random characters
    - Use a third party password manager