HELPFUL HINTS AND ADVICE ON ONLINE HARASSMENT

Online advocacy efforts by human rights organizations face increasingly dangerous threats. These threats aim to damage the credibility of the organization and to limit the public space to advocate on a certain issue, by using rude language on online comments or personally threaten the staff. In this short guide, we elaborate a few helpful hints and advice, as well as list a compilation of resources that organizations can refer to handle online harassment.

WHAT DOES ONLINE HARASSMENT LOOK LIKE?

(PEN America, n.d.)

Online harassment comes in many forms, from individual trolling to organized attacks that are less visible. Knowing the differences will give you more insights to prepare and respond effectively to the attack.

- Trolling: repetitive posting of inflammatory or hateful comments online by an individual whose intent is to seek attention, intentionally harm a target, cause trouble and/or controversy, and/or join up with a group of trollers who have already commenced a trolling campaign.
- Doxing: short for "dropping docs"– this act involves publishing someone's sensitive personal information online to harass, intimidate, extort, stalk, or steal the identity of a target. The information can include social security numbers, phone numbers, home addresses, personal photos, employment information, email addresses, and family members' personal information.
- Cyberstalking: a number of harassing behaviors committed repeatedly or with regularity that usually cause a target to suffer fear, anxiety, humiliation, and extreme emotional distress.
- Online impersonation: where harassers create hoax social media accounts, usually in order to post offensive or inflammatory statements in your name. The harasser's intention is to defame or discredit you, often by convincing others to believe the fake quotes attributed to you, which might then incite others to commit additional acts of harassment. Impersonation trolling can also happen when a harasser impersonates someone you know in order to offend or hurt you.
- Other forms of harassment: hacking, message bombing, etc.

HOW DO I PREVENT ONLINE HARASSSMENT?

Doucet-Bon (2019)[1]

Here are some of the best practices to prevent yourself against online harassment:

- Update your software and applications regularly.
- Create strong passwords. Adopt passwords with at least 16 characters (even when businesses claim less), change them at least every six months and, of course, have different passwords for your mails, Facebook, Twitter, etc. Finally, come up with your own safety questions. Those that are suggested to you are too often bait. Make sure you have not given the answer on a public account.
- Never log into an application via Facebook or Gmail or otherwise.
- Do not give access to your contacts to an application. Allow geolocation only if you deem it necessary. Limit it to the time of use of the application.
- Have an internet application to call like Google Voice, for example.
- Protect yourself against sim jacking. Sim jacking is when a hacker calls your operator pretending to be you, declares that he has lost his phone and requests that the incoming traffic be re-rooted to another sim card, his own. To do this, ask your operator to associate a PIN code to your account to avoid this.
- Use encrypted email: Signal, Telegram, WhatsApp or Wire. Especially if you plan to work on risky topics.
- Protect yourself from doxing. Be careful not to leave any personal information about your biography while attending a conference or other public event. Track your personal information using Google alerts as it will give you notifications if someone shares your information online.

[1] The web page is only available in French.

- **Separate your private life and your professional life**. Choose a platform for your personal life and another for your professional life. In order to clean your accounts, all the couriers now offer easy access to modify your privacy settings. Avoid posting family photos or your house on public accounts.
- **Encrypt your sensitive mails**. Ask your supplier. The easiest: Mailvelope from Gmail.
- **Secure your shipments of sensitive documents.** GlobaLeaks for individuals. You can also suggest your business to use Secure Drop.
- **Secure your VPN**. Two-level security is essential.

This website by the Citizen Lab offers personalized advice to protect your online presence and/or information: https://securityplanner.org.

HOW DO I DEAL WITH ONLINE HARASSMENT?

(Institute For War And Peace Reporting, 2019, p. 210)

Flag the exact comment or post, as recommended by Facebook. Provide as much context as possible in the reporting process. Users may check updates to this process at https://www.facebook.com/report.

Block harassers. This will prevent them from sending friend or follow requests, starting a conversation, sending any messages, and seeing any updates posted to a user's feed. Users are not notified when they've been blocked, but they may still notice that it has happened if they are suddenly no longer able to contact a target.

Report the incident and keep a record of the case number for any follow up action, as recommended by Twitter to users who are the target of online harassment. On Twitter, it is possible to report an individual tweet as well as an entire profile.

Take screenshots before blocking harassers on platforms to keep as documented evidence of abuse. Once they are blocked, it becomes much more difficult to collect supporting evidence, which users may be asked to present during an investigation into the incident.

Start a documentation journal.

- Documentation can be useful for later reference when attempting to **connect the dots between different incidents** that took place during a specific timeframe, or that happened to several people in the same organization.
- Documentation can reveal patterns of abuse or other online attacks you may not have otherwise noticed, by presenting a collated body of evidence – these patterns can be helpful for **identifying adversaries**, or to **draw connections** between certain kinds of incidents and certain actions of yours or your organizations.
- When reporting incidents of abuse on social media platforms, for instance, evidence such as screenshots or profile names may be requested during an investigation.
- **Use this template** for your documentation journal (Institute For War And Peace Reporting, 2019, p. 216):

Date	
Time	
Summary of incident	
Platform	
URL	
Screenshot (filename or copy/pasted)	
Description of screenshot content(s)	

Risk level	*Be sure to specifically expound on the Risk level, as this field is highly subjective and less self-explanatory than the others.*
Follow-up actions	
Notes	

WHERE CAN I FIND FURTHER RESOURCES ON ONLINE HARASSMENT?

Below is a list of further readings to help you handle online harassment:

CITED REFERENCES

Doucet-Bon, P. (2019, Septembre 19). *Journalisme : harcèlement en ligne, ça n'arrive pas qu'aux autres*. Récupéré sur https://www.meta-media.fr/2019/09/19/journalisme-harcelement-en-ligne-ca-narrive-pas-quaux-autres.html

Institute For War And Peace Reporting. (2019). *Holistic digital security training curriculum for wpmen human rights defenders.* Retrieved from https://cyber-women.com/en/cyberwomen/cyberwomen.pdf

PEN America. (n.d.). *Defining "Online Harassment": A Glossary of Terms*. Retrieved from ONLINE HARASSMENT FIELD MANUAL: https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

OTHER REFERENCES

Feminist Frequency. (n.d.). *Speak Up & Stay Safe(r): A Guide to Protecting Yourself from Online Harassment*. Retrieved from https://onlinesafety.feministfrequency.com/en/

Freedom of the Press Foundation. (2019). *Mobile Security Prevention Tips*. Retrieved from https://freedom.press/training/preventative-mobile-security-tips-activists/

Frontline Defenders. (2011). *Workbook on Security: Practical Steps for Human Rights Defenders at Risk.* Retrieved from https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

PEN America. (n.d.). *Online Harassment Field Manual*. Retrieved from https://onlineharassmentfieldmanual.pen.org/

PEN America. (n.d.). *Protecting Information from Doxing*. Retrieved from https://onlineharassmentfieldmanual.pen.org/protecting-information-from-doxing/