Module 3 video 3: Techniques for documenting online abuse

Hi everyone, welcome to the third video of this course Online harassment: journalists' strategies for defense. My name is Ela Stapley, a digital security advisor working with the International Women's Media Foundation (IWMF).

This session will walk you through some practical tips for documenting your abuse, including where to store your documentation and how to record it. But before I do that, let's talk about why it can be important to create a record of what is happening to you.

Documenting abuse is not for everyone. Going through abusive messages can be traumatic and it can also be difficult to identify which threats could result in physical harm, especially if your accounts are being subjected to thousands of attacks a day. So, why document it?

Creating a record of your abuse can be helpful if you need to show others what is happening to you. This can include colleagues, editors, organisations that defend freedom of expression who may be able to support you, and, in some countries, the authorities. Journalists have also documented abuse as a way to look for stories in the data they have collected, for example, repeat abusers who may be linked to government officials.

Documenting can also help you look for patterns in the harassment, such as repeat abusers, and it can also help you keep track of accounts you have reported to social media companies. You will learn more about how to do that in the next module with Myra Abdallah.

If you feel that you are unable to document the abuse by yourself then you should reach out to a friend or trusted colleague who may be able to assist you with it. They may be able to monitor your accounts for you allowing you to take a much-needed break. If you are a colleague or editor and know that someone you work with is a target for online abuse consider reaching out to them to see how you can help. Setting up support networks in the newsroom or between other freelance colleagues can help.

It will not be possible to document every online attack. There are too many of them and often accounts are swamped with so many messages that it renders the account practically unusable. Instead, you should focus on documenting accounts that repeatedly harass you, messages you feel are particularly threatening, or any online threat that may indicate that a physical threat is possible, such as your address being circulated online.

Now, let's look at how to document your online abuse. The first thing you need to think about is where you will store your documentation.

If you are storing information on a shared computer, such as in a newsroom or maybe you are working from an Internet cafe, you ideally do not want to store it in a file on that computer. This is because other people will be using the device and could easily have access to your information. If you do have to store it on a file on a computer you should password protect and/or encrypt it. You should create a name for the file that does not give away any personal details about you or the contents of the file.

You may want to keep your documents in the cloud, for example, in Google Drive. This is a lot more convenient because you can access it from any device. However, you should ensure that your cloud account is protected with a long password and has two-step verification turned on. You will learn how to do that next week in the final module of this course. It is a good idea to encrypt your documents in the cloud, one way to do that is using a tool called Cryptomator. Encrypting your documents in the cloud will better protect them if your cloud account is breached. If you believe that your harassment is coming from a government and that they may subpoena the company for details on the contents of your account then you may wish to avoid storing it in the cloud.

Wherever you decide to store your documentation you should ensure you have a backup copy in case you lose access to the files you have created. For example, on an external hard drive.

The next thing you need to do is to create a spreadsheet. We have provided a template for you in the resources section of this module. The information you store in your spreadsheet should be able to give you and others an overview of the types of harassment you are being subjected to. Think about the data you need to document. It’s a good idea to include the type of harassment, the date of the harassment, the platform where you were harassed, and whether you have reported the abuse to the tech company. This can help you track cases.

You will also need to take a screenshot of the message. It’s important that the screenshot contains all necessary data. Why? Because this is information that can help you identify patterns to the abuse. It is also information that could be requested by law enforcement if you decide to report your harassment to the police. So what sort of information should you capture? It’s important to take a screenshot of the whole message. Make sure you include the handle, that’s the social media name of the abuser, as well as the date and time the message was sent.

As I mentioned at the beginning, documenting abuse is not always easy or feasible. But it may be useful for you, your colleagues, or your newsroom. Get started today by downloading and using our tracking template and you can learn more about documenting abuse in more detail in another of the IWMF online courses, Know your Trolls.