Doxxing: Prevention Tips & Damage Control

1

Simple Prevention Tips

If you do not think you have been targeted, but still want to protect yourself:

- **Search for yourself online and see what you find**
- **Work to isolate/monitor your social media accounts**

2

- Avoid using your full/real name as a username.

- Use separate usernames for accounts you wish to keep separate.

- Work to isolate/monitor your social media accounts

3

- Avoid using gendered usernames ("girlygirl10001") and profile images which contain your face.

- Use a password generator and manager to ensure you have strong passwords for each of your accounts.

- Use a multi-factor authentication (MFA) app

4

- **Avoid “connecting accounts” where possible. For example, many sites will let you sign in using your Facebook account.**

- **Instead, create a separate account where you can.**

5

Privacy Settings

Check your privacy settings for your accounts

limit who is able to see certain information about you and what you post.

If there is a "suggested friends" setting, turn it off.

Hide who likes your posts. Do not allow anyone to tag you without permission.

Do not allow applications to track your location or collect data unless absolutely necessary.

Do not give other ways of contacting you on your public profile.
(phone, email)

6

Advanced Prevention Tips

If you do not believe you have been targeted, but have reason to be paranoid:

- **Instead of following politically radical accounts, it might be wiser to find an affiliated individual who reposts them often and follow this user instead, to avoid direct affiliation between you and the organization online.**

- **Instead of liking politically radical posts, save them. This does more to boost them than favoriting and is not public.**

7

If something involving you gains popularity online, track mentions of your usernames on social media platforms through:

Using a leak checker application/website ("haveibeenpwned.com") and getting an application which requests data removal (Incogni, EasyOptOuts)

Check on who watches your stories regularly, and who follows you, even if they appear to be bots. Many "bots" are either users in disguise, or represent a program used to check on you.

Use an encrypted messenger (such as Signal) as frequently as possible and set a timer for messages to disappear. Use an encrypted email, such as ProtonMail. Use TOR and a VPN when possible.

Do not open links or download unusual attachments from emails unless you are expecting to receive something. Suspicious links/attachments may be malware in disguise.

8

Damage Control

if you have been doxxed/will be doxxed imminently and need to minimize the threat as quickly as possible

Do not engage with antagonistic threats. Deactivate and lock relevant accounts and keep a list of them.

Log all incidents related to the doxxing. What photos were leaked? What information? What was the username of the person/ organization who posted them?

If you know a hostile individual or group has taken issue with your post, it may be a good idea to follow them via a burner account.

For all incidents which take place online, use the platform’s “report” function whenever possible and encourage others to report the offending post as well.

9

Turn your phone to airplane mode or off when heading somewhere you do not want to be tracked. Do not use phone calls for sensitive conversations.

10

Damage Control

If You Are A Student or Corporate Worker

- Do not list your school/company affiliation on your accounts. Do not mention it by name at all.

- If you are requested to give your social media handles by your institution or organization, refuse if possible. If not, say that you do not have an account on that platform.

- If necessary, have an account you do not use for regular activity which you give for this purpose.

- Do not sign up for accounts using your school/work email address.
- Do not browse the internet while logged into a school/work Google account.
- Have your name removed from any public directories online.

- Do not location tag venues or tag groups related to your school or work on social media.

- Do not follow accounts associated with your school or work.

- If you have an uncommon name, avoid using the full version in your private social media profiles.

Possible Venues For Surveillance

If you are a Palestinian activist or part of an active group for Palestine

Interrogation by authorities

Raids - Searches

Posts on social accounts

photo databases (Blue Wolf)

Facial recognition cameras

CCTV cameras

- Monitored telephone calls
- Location tracking/data stealing spyware (Pegasus)

7amleh.org

www.partnersglobal.org

The Gaza War Response Resources are created as a collaboration between a number of organizations.

WITNESS SEE IT FILM IT CHANGE IT

SMEX

Meedan

حـمـلـة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center For
the Advancement of Social Media