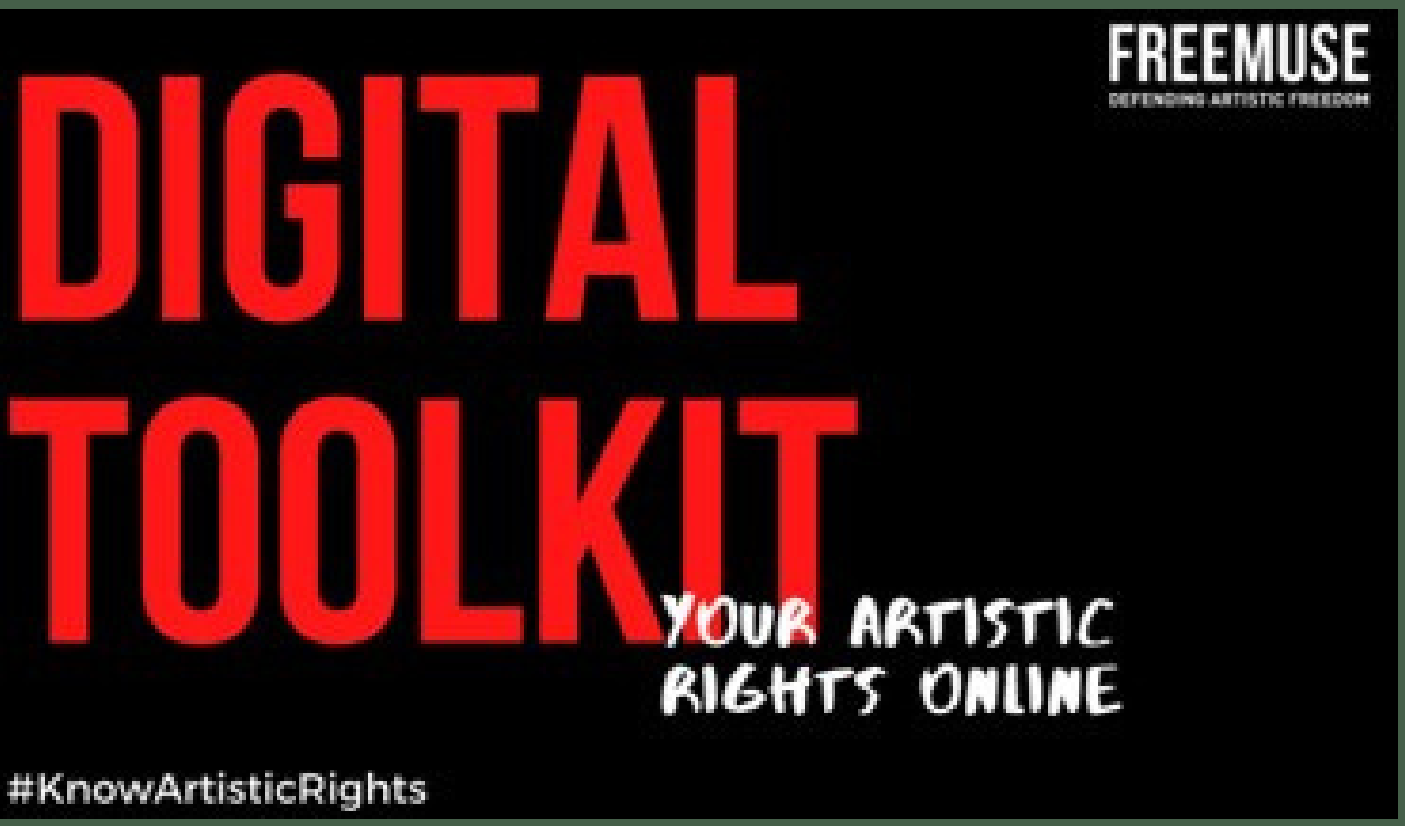
WHAT TO DO WHEN YOUR DIGITAL RIGHTS ARE VIOLATED?



FREEMUSE
DEFENDING ARTISTIC FREEDOM

Set your boundaries

FREEMUSE
DEFENDING ARTISTIC FREEDOM

Remove personal information

- Make your social media accounts private
- Delete available information that might endanger you

Document the incident

- Keep record of the attacks
- Collect visual evidence of the incident: date, time, pictures, number of threats, people involved.
- Keep the evidence safe

Report the incident

<u>To social networks:</u>

a- Facebook and Twitter have an inbuilt function to flag offensive and hateful comments

b- through the provided channels if your account was taken

c-Relevant channels

<u>To the police:</u>

Especially relevant in doxing.

<u>To someone you trust:</u>

If the situation affects your mental health, rely on someone you trust to monitor and report

Block, mute, delete accounts

- Beneficial in some cases of threats and hate speech but has to be avoided to monitor the harasser's activity and prevent the loss of evidence
- You can use third-party apps to block accounts like those already on your block list, like Block Together

Reclaim the narrative

- Spread awareness through fact-checked information to alert your network of any inaccuracy
- Avoid fueling trolls by using inflammatory language and insults.

Update digital safety

- Secure your accounts and passwords
- Contact relevant providers if information was stolen
- Check if any program or virus was used to obtain personal information from devices - more info in Safe Sisters Guide.

Gain security and support

FREEMUSE
DEFENDING ARTISTIC FREEDOM

Take a break from online spaces and social media platforms

when harassment negatively impacts your mental and physical health

Assess the risks and consider relocating

If the attacks extend to offline spaces (notably common in doxing or hacking)

Document evidence and Seek legal advice

when circumstances reach a critical point

Seek Further Protection

FREEMUSE
DEFENDING ARTISTIC FREEDOM

Protect your identity

Monitor the online information about your personal life:

1- By using google alerts to get an email/notification whenever your query shows up on the web.

2- By educating family and friends on the importance of sharing personal information online because one hacked account puts everyone in the network at risk of hack or attacks.

Location

1- Disable all geo-location settings and upload pictures/videos after leaving a location rather than in real time.

2- Use VPN technology

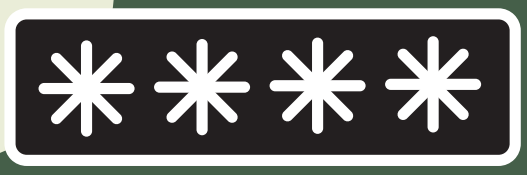
Camera and liverstreaming

1- Reverse image search to identify the source of the visual when monitoring your unwanted online presence.
2- Cover your cameras with stickers or paper when they are not in use.

3- More expensive camera covers include C-Slide and SpiShutter.

4- Opt for applications that allow for blurring of faces and information when recording visuals, like ObscuraCam v1.

Username and passwords



1- Don't use the same username and password for every site
2- Use multi factors/2 step authentication when logging in
3- When choosing passwords and secret questions, make sure that the information cannot be found on your social media accounts(birthday or cat name), and consider the following:

a- using password managers (LastPass and Dashlane)and password generators (Password Generator)

b- using a randomly generated answer in response to secret questions.

c-using a passphrase rather than a password

Email and social media accounts

1- Create an account in your name on all main online platforms
2- Create public social media pages for artistic work and private accounts for personal networks.
3-Inspect the privacy setting of each site
4- Create separate email accounts for different purposes.

Website security

1- Install widgets and plugins from safe sources
2- Moderate or turn off comments
3- Use services that offer automatic backups when websites are attacked like VaultPress or BackupBuddy.
4- Start protecting your website against a DDoSattack by going through the questions on DigitalDefenders.org.

Operating systems

1- Select the highest privacy settings on all apps, platforms, and sites.
2- Install an anti-spyware software (free software include Spybot and ad-blockers)
3- Install an anti-virus software
4- Constantly update your operating systems

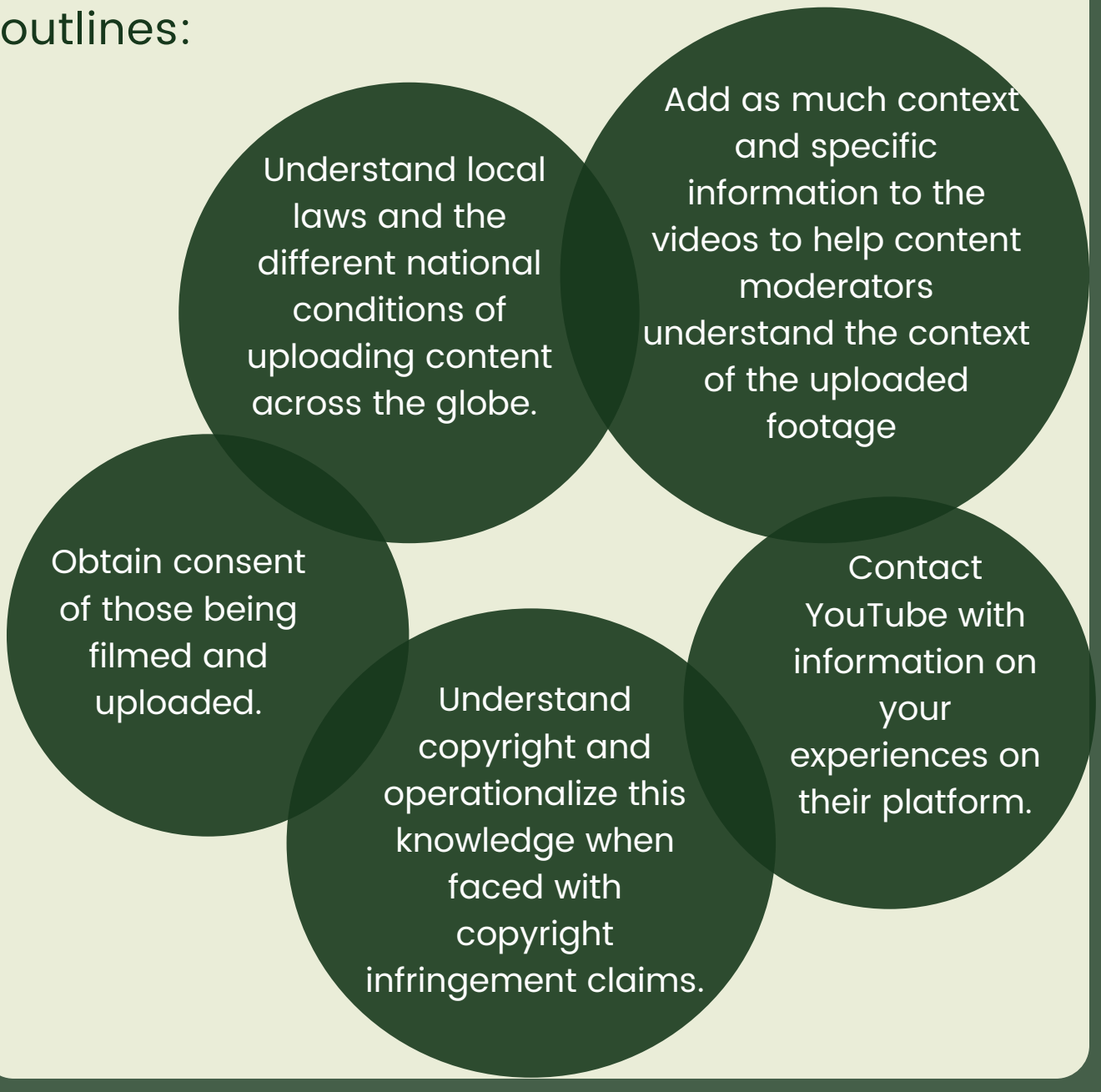
Access to devices

1- Always set up a PIN code
2- Delete browser history and sign out of all your accounts, if you're using a device that's not yours.

Videos

1- Respect the online platform's community guidelines

2- On protecting videos on YouTube, "WITNESS" outlines:



Recognize phishing attempts

Some basic ways to avoid phishing (by Phishing.org):

1- Keep informed about phishing techniques and new scams.

2- Do not click on links that appear in random messages or emails. If you are unsure about the origin or contents of a link or attachment, do not click and go to the source for more information.

3- Be cautious with pop-up windows as they often serve as phishing attempts. Click on the ‘x’ rather than ‘cancel’ when they appear.

4- Install an anti-phishing toolbar on your computer.

5- Verify websites' security and only visit encrypted pages.

6- Regularly change your passwords.

7- Keep your browsers updated.

8- Install firewalls to function as a buffer between your computer and the outside world.

9- Never share personal or financial information over the Internet.

10- Use antivirus software.

Additional resources

FREEMUSE
DEFENDING ARTISTIC FREEDOM

SMEX:
https://smex.org/
SMEX Helpdesk: https://smex.org/helpdesk/

WITNESS
https://technology.witness.org/

Take Back the Tech:
https://www.takebackthetech.net/

Cyberbullying:
https://cyberbullying.org/

Crash Override:
http://www.crashoverridenetwork.com/

Without My Consent:
https://withoutmyconsent.org/

The Weather Report:
http://www.theweatherreport.org/

Crash Override: Guides and other resources:
http://www.crashoverridenetwork.com/resources.html

Fundación Karisma: Become INTERNET GENIUS … Renewed:
https://web.karisma.org.co/pagina-principal-2/our-work/campaigns/become-internet-genius-renewed/

PEN America (https://pen.org/):
Visit their online harassment manual:
https://onlineharassmentfieldmanual.pen.org/

IFEX digital security
https://ifex.org/ar/

7amleh:
https://dsc.7amleh.org/

Anti-Defamation League, Responding to Cyberhate –Toolkit for Action:
https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/ADL-Responding-to-Cyberhate-Toolkit.pdf

Haystack Project:
https://www.haystack.mobi/

Internet Lab:
https://www.internetlab.org.br/en/biblioteca/

Justitia:
http://justitia-int.org/en/new-report-digital-freedom-of-speech-and-social-media/

Gender and tech resources:
https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

Steph Guthrie, TEDx talk: The problem with don't feed the trolls
https://www.youtube.com/watch?v=_KHEkR5yb9A

Front Line Defenders
https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

EFF:
https://ssd.eff.org/en/module/creating-strong-passwords

Cloudwards:
https://www.cloudwards.net/dashlane-vs-1password/

Safe Sisters (https://safesisters.net/)
A common sense guide to digital safety for women and girls in Sub-Saharan Africa: https://internews.org/wp-content/uploads/legacy/2018-09/Safe-Sister-Guide.pdf

Access Now:
https://www.accessnow.org/help-ar/?ignorelocale

Online Safety: Speak Up & Stay Safe(r):
https://onlinesafety.feministfrequency.com/en/

TrollBusters (http://www.troll-busters.com/)- Their infographic: Are you being harassed online?
https://yoursosteam.files.wordpress.com/2017/01/tb_infographic_watermark.jpg