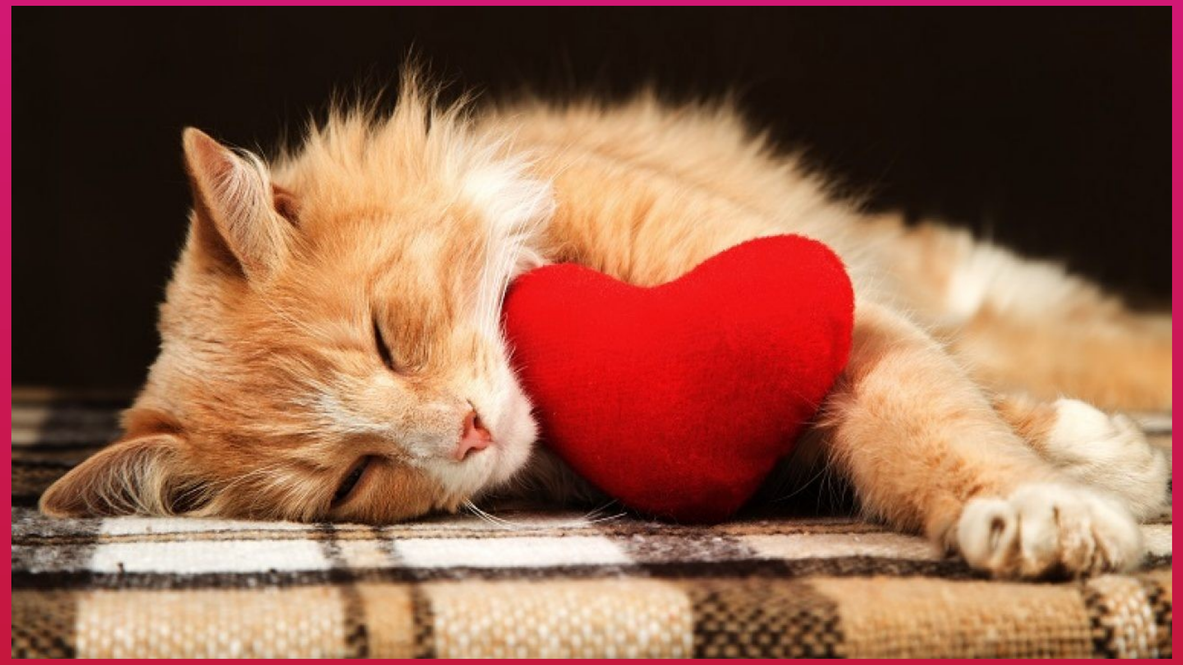


Cyber Harassment + Harm Reduction

BROOKLYN INFOCOMMONS
FEBRUARY 20 2021
EXP 08/21

CyPurr Collective

OVERVIEW

Intro

Special Guest- Eva Galperin

Cyber Harassment + Harm Reduction

Outro

(Cypurr After Hours)

WHO ARE WE?

We are...

The Cypurr Collective: A group of folks that organize cybersecurity events, looking to spread knowledge and talk about privacy rights!

Established April 2016

Just some folks interested in making safer spaces for others to talk bout their privacy needs

A FEW RULES FOR THE SPACE

Saf(er) Space - We **DO NOT** tolerate language or behavior purposefully meant to demean or harm folks based on their identities

Share the space - Feel free to ask questions in the chat!

- Cypurr folks on standby
- Will answer questions relating to topic on main, private message for other questions
- More time to talk during after hours!

A FEW RULES FOR THE SPACE

Photo/Video - Slides/Resources available after! Video available soon.

A note on voice recording…

We are trying to keep these presentations for posterity, and not to record participants. We will try to anonymize people when possible but please be aware that we are recording and may need to keep voices in the audio for context. **Use the chat if possible for questions and discussions if you do not want your voice on the recording.**

AND NOW...

EVA GALPERIN

Director of Cybersecurity at the Electronic Frontier Foundation

Cypurr Session:
Cyber Harassment and Harm Reduction

2/20/21
@ 2 PM

Brooklyn InfoCommons
Zoom

Content Warning

This workshops discusses or mentions issues around intimate partner violence a.k.a domestic violence, as well as stalking and harassment

What do we mean by Cyber Harassment?

Cyber Harassment, “is a catch-all term for various tactics and malicious behaviours online. This ranges from sharing embarrassing or cruel content about a person, impersonating, doxing and stalking, to the nonconsensual use of photography and violent threats. The purpose of harassment differs with every incidence, but usually includes wanting to embarrass, humiliate, scare, threaten, silence, extort or, in some instances, encourage mob attacks or malevolent engagements.”

-Glitch

What do we mean by Harm Reduction?

"**Harm reduction**, or harm minimization, refers to a range of public health policies designed to lessen the negative social and/or physical consequences associated with various human behaviors, both legal and illegal. Harm reduction policies are used to manage behaviors such as recreational drug use and sexual activity in numerous settings that range from services through to geographical regions."

-Wikipedia

Stats on Cyber Harassment

Pew Research Study (2017)

Overview

Scope: Estimated 7/10 U.S. adults use social media (around 250,000,000)

In 2017, Pew Research conducted a survey, looking to understand the scope, severity, and subjectivity of online harassment

A study of 4,248 U.S. adults finds that

- 41% of Americans have been personally subjected to harassing behavior online, a modest increase from 35% [of a similar Pew Survey from 2014]
- 66% have witnessed these behaviors directed at others

Stats on Cyber Harassment

Pew Research Study (2017)

Identity

- Race
  - one-in-ten have been targeted due to their physical appearance (9%), race or ethnicity (8%) or gender (8%)
  - one-in-four Black folks say they have been targeted with harassment online because of their race or ethnicity, as have one-in-ten as have one-in-ten Hispanics. The share among whites is lower (3%).
  - while Black folks (74%) and Latinos (72%) are more likely to say that online harassment is a major problem compared with whites (57%).

Stats on Cyber Harassment

Pew Research Study (2017)

- Gender
  - women are about twice as likely as men to say they have been targeted as a result of their gender (11% vs. 5%)
  - Some 21% of women ages 18 to 29 report being sexually harassed online, a figure that is more than double the share among men in the same age group (9%).
  - 53% of young women ages 18 to 29 say that someone has sent them explicit images they did not ask for.
  - half of women say offensive content online is too often excused as not being a big deal, whereas 64% of men – and 73% of young men ages 18 to 29 – say that many people take offensive content online too seriously.
  - 70% of women – and 83% of young women ages 18 to 29 – view online harassment as a major problem, while 54% of men and 55% of young men share this concern.
  - Fully 83% of women ages 18 to 29 describe online harassment as a major problem, a substantially larger share than either men in the same age group (55%), women 30 and older (66%) or men 30 and older (53%).

Stats on Cyber Harassment

Amnesty International Survey

- Around 4,000 women between the ages of 18 and 55 in Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and USA.

- 23% of the women surveyed across these eight countries said they had experienced online abuse or harassment at least once

- 41% of women who had experienced online abuse or harassment said that on at least one occasion, these online experiences made them feel that their physical safety was threatened.

- 46% of women responding to the survey who had experienced online abuse or harassment said it was misogynistic or sexist in nature.

- Between one-fifth and one-quarter of women who had experienced abuse or harassment said it had included threats of physical or sexual assault.

- 58% of survey participants across all countries who had experienced abuse or harassment said it had included racism, sexism, homophobia or transphobia.

Types of Cyber Harassment

Online Hate Speech

“Online hate speech has no uniform legal definition but can be found in different statutes. The baseline definition is expressions whether that is written material, action and images of hatred toward someone on account of that person’s colour, race, disability, nationality (including citizenship), ethnic or national origin, religion, or sexual orientation, disability or other traits.” -Glitch (via Women’s Media Center)

Note: For this workshop, we will be looking at the effects of hate speech on historically marginalized identities including gender (women, trans folks, nonbinary folk), race (black, indigenous and people of color or BIPOC), sexuality (LGBQTAI folk), size, disability, occupation (sex workers) and any combination of these identities, within a U.S. context. Although, hate speech is not solely applicable to the mentioned identities.

Also this presentation won’t be getting into the issue of how hate speech is moderated.

Types of Cyber Harassment

Trolling

“The act of causing problems on the internet by starting arguments or upsetting people, by posting inflammatory messages. It is done with the deliberate intent of provoking readers into an emotional response”- Glitch (via Women’s Media Center)

Types of Cyber Harassment

Cyberstalking

"The use of the internet of other electronic means to stalk or harass an individual, group or an organisation.”- Glitch (via Women’s Media Center)

This could include the monitoring of electronic devices (i.e. mobile, desktop and/or internet of things), as well as contact through social media and/or online channels,

Types of Cyber Harassment

Spyware

applications used to siphon user data from a device, mobile or otherwise. This type of application is typically used found within contexts of state use for covert operations, employers monitoring their employees, parents monitoring their children, or intimate partner violence.

Stalkerware

“…spyware that is explicitly sold or licenced to facilitate intimate partner violence, abuse, or harassment, inclusive of deleteriously intruding into the abused partner’s private life by way of physical or digital actions, as stalkerware by definition. We also stipulate that spyware operates as stalkerware when surveillance software sold for ostensibly legitimate purposes (e.g., monitoring young children or employees) is repurposed to facilitate intimate partner violence, abuse, or harassment. To be clear, this means that even application functions included in mobile operating systems, such as those which help to find one’s friends and colleagues, can constitute stalkerware under certain circumstances.” - Citizen Lab *Predator in Your Pocket*

Types of Cyber Harassment

Doxxing

“The unauthorised retrieving and publishing, often by hacking [but also through publicly available means] of a person’s personal information, including, but not limited to, full names, addresses, phone numbers, emails, spouse and children names, financial details. ‘Dox’ is a slang version of ‘documents’ or .doc. Causing fear, stress and panic is the objective of doxing, even when perpetrators think or say that their objective is ‘harmless’.” Glitch (via Women’s Media Center)

Types of Cyber Harassment

Revenge Porn

“The distribution of sexually graphic images without the consent of the subject of the images.” Glitch (via Women’s Media Center)

Distribution can be achieved, for example, through social media applications, phone applications, text messages, and/or posted on websites or blogs.

Types of Cyber Harassment

Deepfakes

"The term deepfake was first coined by the Reddit user u/deepfakes, who created a Reddit forum of the same name on November 2nd 2017. This forum was dedicated to the creation and use of deep learning software for synthetically faceswapping female celebrities into pornographic videos. Since Reddit's removal of /r/Deepfakes on February 7th 2018, deepfakes have become increasingly commodified as new deepfake forums, tools, and services have emerged."

-Deeptrace *The State of Deepfakes*

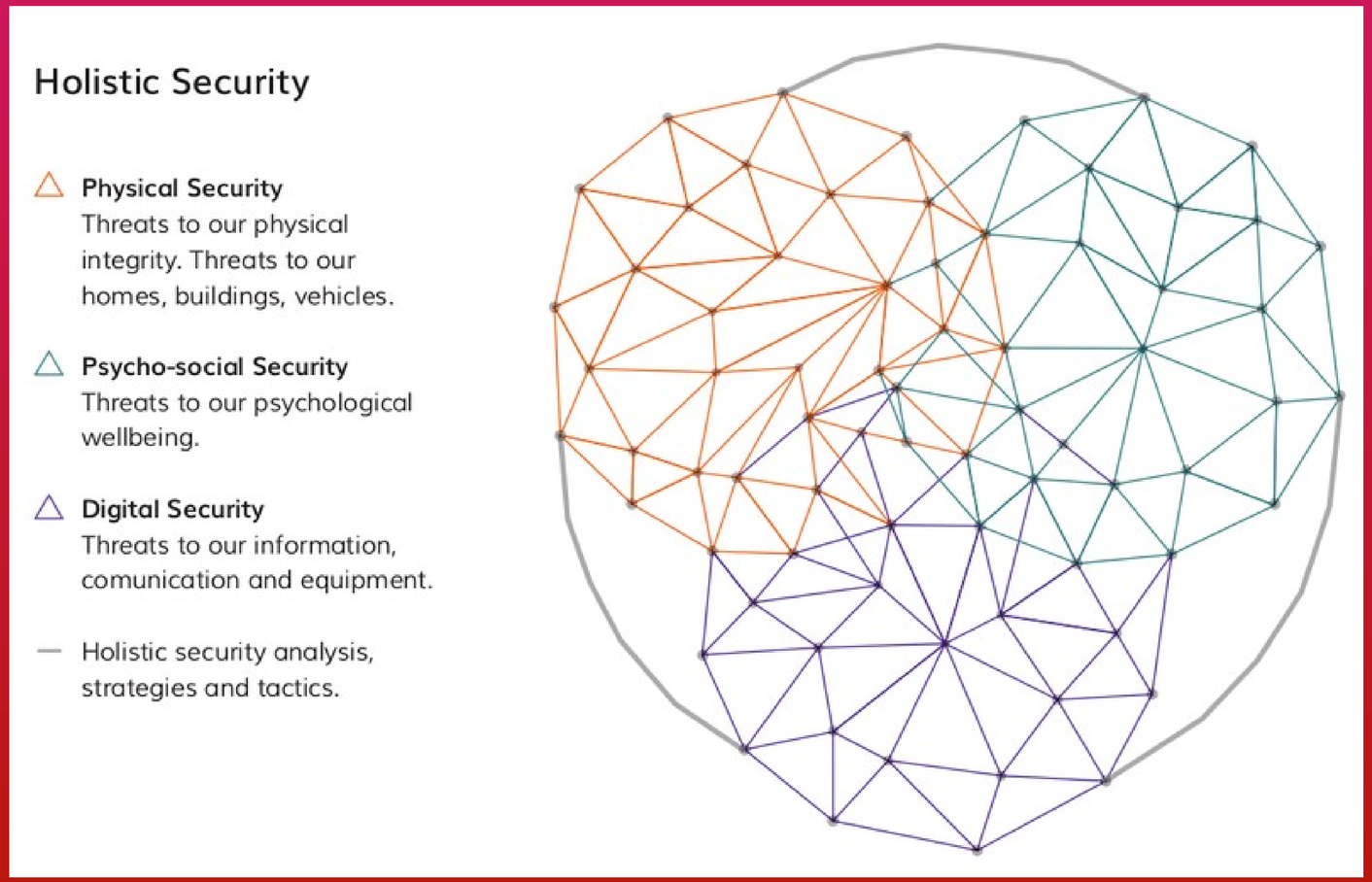
ADDRESSING CYBER HARASSMENT

ADDRESSING CYBER HARASSMENT

General Tips

Holistic Security

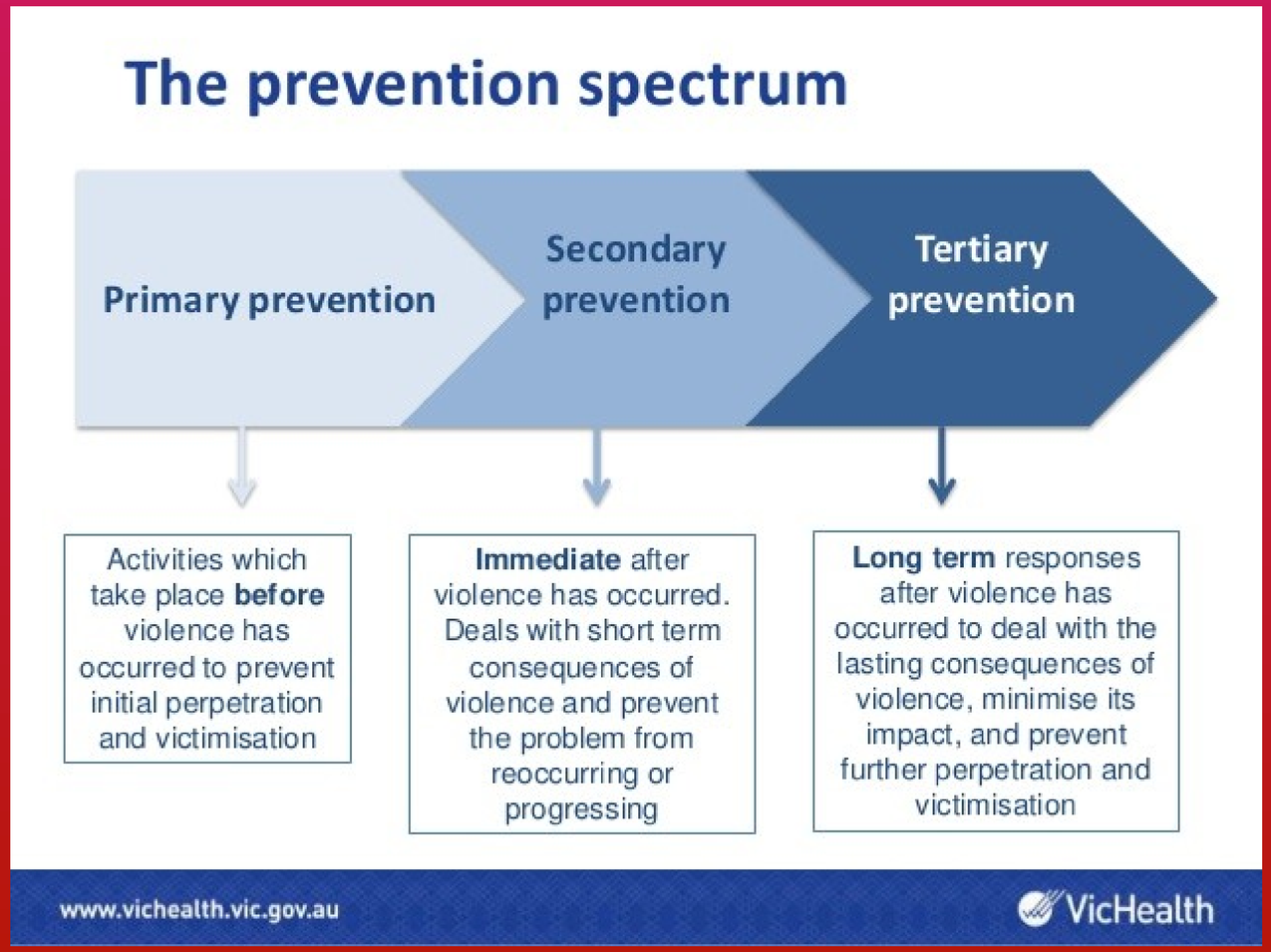
- Tactical Tech Collective
- Our digital security is linked to our physical and emotional security
- Addressing one helps all!



ADDRESSING CYBER HARASSMENT

General Tips

- Make a plan-
  - Before
    - Gather community
  - During
    - Trust your instincts
    - Look for patterns
    - Document Incident
  - After
    - Report Incidents
    - Activate support systems



ADDRESSING CYBER HARASSMENT

Strategies

Public Profiles

- Examining intentions around social media
- Raising self-awareness around your digital-self
  - Public/Private
    - Understanding what you post and who can see
    - Learning about the privacy options available to you per platform
  - GeoTagging
    - being aware of location data posted by you or others
  - Friends/Acquaintances/Blocks
    - Understanding who follows you
  - Who has access?

See: Zebra Crossing guide in resource page for more!

ADDRESSING CYBER HARASSMENT

Strategies

Devices (Phones/laptops/IoT)

- Who has access to my devices (physical/digital) ?
- Do I recognize the apps on my device?
- How should my device act normally? Is it doing anything unusual?

ADDRESSING CYBER HARASSMENT

Strategies

Password

- Password Manager
  - Multiple, complex passcodes
  - I.e. BitWarden, KeepassX
- 2FA
  - Two Factor Authentication
  - Allows for second line of defense for your profiles

We'll be talking more about passwords at our next Cypurr Session on March 20th!

ADDRESSING CYBER HARASSMENT

Strategies

Information Awarness

- Search Engines
  - What info of your is out there?
- Data Brokers
  - What sites are publishing more personal information of mine?

Note: See Big Ass Data Broker Opt Out List in our resources list for more information on sites and removal

ADDRESSING CYBER HARASSMENT

Strategies

Documentation

(via Tech Safety)

- Keep a log of all incidents,
- Save everything related to the event or incident.
- Think about technology that you suspect the abuser could be using.
- Think about your safety first.
- Document only relevant information.

What to Document

- Email
- Text Messages
- Social Media/Internet Harassment
- Harassing Phone Calls
- Phone Number/Caller ID Impersonation

ADDRESSING CYBER HARASSMENT

Online Hate Speech/Trolling

Apps

- **Block Party-** “Use Block Party to filter out unwanted @mentions from Twitter, and continue to use Twitter as normal.”

Services

- **HeartMob**- “HeartMob... aims to be the place where those facing harassment can easily report abuse across social networks and find support from others who know what they're going through” — The Washington Post
- **Games and Online Harassment Online**- The Games and Online Harassment Hotline is a free, text message-based, confidential emotional support hotline.

ADDRESSING CYBER HARASSMENT

Cyberstalking

- **Crash Override Network**- List of resources in addressing cyber harassment, including the COACH helper tool
- **HackBlossom-** Scenario-specific guides on how to navigate cyber harassment by a partner
- **Online Safety by Feminist Frequency**- Guides on protecting yourself from harassment online, as well as overviews of strategies and approaches
- **Tiny Kat Cafe-** Guide for Handling Online Harassment
- **Tech Safety** by National Network to End Domestic Violence

…check out more on our Resource List for this workshop!

ADDRESSING CYBER HARASSMENT

Stalkerware

(via **Coalition Against Stalkerware**)

- **Most likely from someone you know** (i.e. partner, family member)

- **Some potential signs of Stalkerware:**
  - Mobile phone, device or laptop goes missing and reappears
  - Lending your device for an extended period of time to someone and noticing changes in settings or unknown apps you do not recognize.
  - Unexpected battery drain (Android and iOS devices)
  - Unfamiliar app or process is on your device.

Also possible to keep track of people using shared accounts/cloud accounts (i.e. Google Maps, Find My Phone)

ADDRESSING CYBER HARASSMENT

Stalkerware

AntiVirus Companies + Stalkerware

- Kaspersky
- Avast
- Malwarebytes
- Lookout

“**Important to Note**: If you delete stalkerware, whoever installed it would know that it’s been disabled. So it’s important to understand that before taking any action, and to have a safety plan ready. One of the points of this plan may be: contact organizations working with victims of domestic violence.” -Coalition Against Stalkerware

See our resource page for more information on organization who work with folks
in intimate partner violence situations

ADDRESSING CYBER HARASSMENT

Doxxing

Doxxing: Tips To Protect Yourself Online & How to Minimize Harm (EFF)

- Plan
  - Take a look at the information that is already publicly available about you online
    - Make a list of accounts
  - Identify who you can trust with your secrets
  - Read up on the policies your online accounts have
- Minimizing Your Publicly Available Data
  - **DeleteMe-** https://joindeleteme.com/
  - **Privacy Duck**- https://www.privacyduck.com/

FURTHER RESPONSES TO CYBER HARASSMENT

FURTHER RESPONSES TO CYBER HARASSMENT

Dealing with Companies

Pros

- a community effort to report a profile or post can help
- More effort into moderation than previously by companies
- Guides at CyberCivilRights.org/online-removal

FURTHER RESPONSES TO CYBER HARASSMENT

Dealing with Companies

Cons

- lack of transparency and investment in the moderation process may not always bring relief to people receiving harm
- Depending on the platform, may be easy for harassers to make new accounts

Ilustration by Corey Brickley

“Roughly half of those who have had untrue information about them posted online have attempted to get it corrected or removed; about seven-in-ten were successful, though many found the process difficult”

-Pew Study

FURTHER RESPONSES TO CYBER HARASSMENT

Law Enforcement

Pros

- In some cases, individuals who seek help from law enforcement on issues of stalking receive helpful assistance in distancing from harasser
- Having a police report may assist in your situation when interacting with sites/platforms

FURTHER RESPONSES TO CYBER HARASSMENT

Law Enforcement

Cons

- A lot of valid reasons why people don’t go to law enforcement
- “Around 1/3 of women in the UK (33%), USA and New Zealand (32%), stated the police response to abuse online was inadequate.”- Amnesty International report on women facing online abuse
- “Almost half (49%) of those who have experienced some type of harassing behavior – including 55% of those who have experienced severe types of harassment – feel that law enforcement does not take online harassment incidents seriously enough.” -Pew Study

“I wish I could say with confidence to a victim, ‘They’ll take you seriously and treat you with respect, and put all of this in a record so they can help you,’”

Dr. Mary Anne Franks, Cyber Civil Rights Initiative Vice-President and Legislative & Tech Policy Director

FURTHER RESPONSES TO CYBER HARASSMENT

Legislation/Litigation

Pros

- Growing understanding from courts/policymakers on the severity of these issues
- More states implementing laws to protect citizens from revenge porn and stalkerware
- Lawyers can help send DMCA takedown notices to websites, file restraining orders

Cons

- Litigation can be costly
- Judicial agents (judges, lawyers) still need to be more informed on the effects of cyberharssment, and the technology surrounding it.

Summary

- It’s not your fault- Not a new issue, but also a new issue
- Community Care- You’re not alone
- Digital Hygiene- Make a plan
- Holistic Security- balancing digital self-defense with emotional and physical defense

Summary

- Tiny Kat Cafe
  - What You Can Control
  - What You can Get Help With
  - What You Can Let Go

THANK YOU FOR WATCHING

FURTHER RESOURCES

Cypurr Resources

Website- https://cypurr.nyc

Open Collective (Donation/Tshirt)- https://opencollective.com/cypurr-collective

Questions? Comments? Topic Ideas?

- Email- cypurr@protonmail.com
- Join our email list for updates!

Social Media- FB/Twtitter @cypurrnyc