Supplemental material for "There's so much responsibility on users right now:" Expert Advice for Staying Safer From Hate and Harassment

1 RECRUITMENT FORM

Subject: Participate in Expert Interviews About Combatting Online Harassment

Dear recipient,

[ANONYMIZED] is exploring a prioritized set of recommendations to help people prevent and mitigate online hate and harassment. To help come up with recommendations, we're reaching out to experts like you. We intend to target these recommendations to adult Internet users broadly. Recommendations might address topics such as:

- Toxic content (bullying, sexual harassment, threats of violence)
- Content leakage (doxxing, non-consensual image exposure)
- Impersonation (deep fakes, fake profiles)
- Available resources (communities, advice guides, legal)
- And more

Given your expertise in this space, would you be willing to participate in an up to 90 minute virtual interview with us on how you think adults can stay safer from hate and harassment online? To thank you for your time and effort, you will receive a $100 gift card for participating.

Interviews are being scheduled for weekdays in July. If you are interested in participating, please fill out this form: [ANONYMIZED]. (You may also use this form to opt-out of being contacted again if you are not interested in participating.)

If you are unable to participate, please feel free to forward this email to other experts you think could provide helpful advice for preventing and mitigating online hate and harassment, or let us know if there is anyone else that you recommend we reach out to.

Please contact [ANONYMIZED] with any questions or feedback.

We appreciate your time and consideration,
[ANONYMIZED]

2 CONSENT FORM

1. Purpose. We are pleased to invite you to participate in a user research study ("Study") conducted by [ANONYMIZED]. The purpose of the Study is to help [ANONYMIZED] better understand [ANONYMIZED].

2. Participation. By participating in the Study you confirm: (a) you are over eighteen (18) years old; and (b) participating in the Study will not violate any agreement with a third party or create a conflict of interest. Your participation in this Study is completely voluntary. You may choose to withdraw at any time during the Study without any penalty. You may also decline to answer any particular question you do not wish to answer for any reason. The researchers also have the right to end the Study at any time.

3. Incentives. To thank you for your time and effort in participating in the Study, you will receive the incentive described in the screener form.

4. Feedback. During your participation in the Study, you may provide comments, feedback, ideas, reports, suggestions, data, or other information to [ANONYMIZED]. For clarity, Feedback is separate from and not part of the Study data. [ANONYMIZED] may use any Feedback without any obligations or restrictions to [ANONYMIZED]. You agree that you will not disclose to [ANONYMIZED] any third-party information that you are otherwise obligated to maintain as confidential. [ANONYMIZED] has no obligation to use your Feedback.

5. Personal Information.

5.a Personal Information Collection Consent.

With your consent, and solely for the Purpose, we may collect and process information that can identify you, including your name, email, and job title, in accordance with this agreement and the [ANONYMIZED PRIVACY POLICY]

I give my consent (initial here): _____

5.b Audio/Video/Photography Collection Consent. This study may involve collecting audio, video, or photographs of you and your interactions with [ANONYMIZED]. For example, we may ask you to remotely share your device screen with the researchers to observe your interaction with [ANONYMIZED]. With your consent, and solely for the Purpose, we may record your face, voice, physical features, mannerisms, likeness, and interactions during the Study session, in accordance with this agreement and the [ANONYMIZED PRIVACY POLICY].

I give my consent (initial here): _____

6. Study Data

6.1 Use and Sharing. Solely for the Purpose, we may: (A) use Study data containing your personal information, including audio, video, or photographs of you, as applicable; and (B) share that Study data with: (i) [ANONYMIZED] and (ii) [ANONYMIZED] who agree to meet our standards for protecting Study data and who have a need to access the Study data for the Purpose.

6.2 Retention. If collected, we may retain your personal information in the Study data only as long as it is necessary for the Purpose. All other Study data that does not personally identify you may be used for any purpose without any limitation.

7. Data Transfer. You consent to [ANONYMIZED] processing Study data outside the country or region where the data is originally collected or where you are located, including in countries where you may have fewer rights about your information than you do in your country of residence. We may process Study data in [ANONYMIZED] or permit [ANONYMIZED] to process Study data outside of your country of residence.

8. Data Storage and Protection. We respect your privacy and use a variety of measures to protect your personal identifying information from unauthorized access and disclosure in accordance with [ANONYMIZED PRIVACY POLICY].

9. Sharing with Third Parties. [ANONYMIZED] may want to share the Study data that personally identifies you with certain third parties such as [ANONYMIZED] who agree to meet our standards for protecting Study data and who have a need to access the Study data in furtherance of the Purpose.

10. [ANONYMIZED] Confidential Information. This agreement and any information provided to you by [ANONYMIZED] during the Study are confidential (the "Confidential Information"). You agree to (i) use Confidential Information only for participation in the Study, (ii) take reasonable degree of care to prevent any unauthorized use or disclosure of Confidential Information, and (iii) not photograph, record, or share any Confidential Information with anyone. Your duty to protect [ANONYMIZED] Confidential Information expires five years from disclosure.

11. Questions/Requests for Deletion. If you have questions or wish to have your personal data contained in the Study data deleted, please email us at [ANONYMIZED]. The subject of your email should be [ANONYMIZED] and your email should include enough information (location, date, time, etc) so that [ANONYMIZED] can identify the Study data collected from you (if applicable). Study data that contains or is linked to your personal information will be deleted as soon as reasonably practicable, unless otherwise prohibited by applicable legislation or legal process. [ANONYMIZED] may, in its sole discretion, retain Study data that does not personally identify you for a longer duration or for any future study.

General Provisions. Unless applicable law requires otherwise: (a) this agreement is governed by the laws of [ANONYMIZED]; and (b) the exclusive venue for any dispute relating to this agreement will be [ANONYMIZED]. Any amendments must be in writing. Failure to enforce any of the provisions of this agreement will not constitute a waiver. This agreement does not create any agency or partnership relationship. If any term (or part of a term) of this agreement is invalid, illegal or unenforceable, the rest of the agreement will remain in effect. This section will survive any termination of this agreement. You can contact your local data protection authority if you have concerns regarding your rights under local law.

Full Name: _____

Signature: _____

Email Address: _____

Date: _____

3 INTERVIEW SCRIPT

Introduction

Hi, I'm [name of primary interviewer], and I'll be leading our research session today. [Name of second interviewer] is also here to take notes and has their camera on now to say hi and so you know who else is here.

Thank you so much for participating in this interview. Our goal is to understand what advice you would give Internet users to prevent or minimize their exposure to online hate and harassment.

So the schedule for today – I'll start by asking about your background and expertise on this topic. Then, we'll have a couple of interactive activities. And at the end, we'll have some high-level wrap-up questions. We estimate this will take about 90 minutes. Do you have a hard stop today?

Please keep in mind that this is not an evaluation of you or your experiences. For the purposes of this research study, there are no right or wrong answers — our goal is to learn from you and to understand your experiences and perspectives.

I also want to say that your participation in this study is voluntary. We are going to be talking about hate and harassment, which can be a difficult topic. You can stop or take a break at any time. If you don't want to talk about or perform any action, just let me know, and we will move on. Any questions for me before we start?

And can I verify that you signed the consent form?

Is it okay with you if this interview is recorded? The recording will only be shared with the research team and will be deleted when the research is complete.

Expert background and personal expertise

First, I'd like to ask you about your personal expertise in this topic. What experiences or roles have you held related to the broader aim of studying or stopping online hate and harassment?

Follow-up questions, if not already mentioned by the participant:

- How often in your day-to-day do you advise individuals on how to stay safer from online hate and harassment?
- Are there any specific groups of people you have the most experience assisting (activists, LGBTQ+, journalists, teens)?
- How long have you been working with or supporting people experiencing hate and harassment?
- How did you come to this work?

Threat ranking

This first activity is about which types of hate and harassment you think the general internet user should prioritize taking action to mitigate or prevent.

I'm about to put a link to the tool we'll be using for the interactive activities into the chat. Please open it in your browser and present the screen with that window. Take your time, sometimes getting the permissions set up can be complicated, just let me know how it's going.

On the left, there are 7 categories of online hate and harassment. So the question for this activity is, for a general internet user who is not experiencing an attack right now, which threats should be their top priority for trying to mitigate or prevent? Drag the cards on the left into order in the box on the right.

There are no right or wrong answers here – we're just interested in your perspective of ranking these threats. To that end, please speak your thought process aloud as much as possible to help us understand what you're doing and why.

Follow-up questions, if not already mentioned by the participant:

- Why did you put this category at the top?
- How was your ranking here, for a general internet audience, informed by the population you are most familiar with? Do you think your ranking of threats would change for a different population?
- [*Summarize reasons that participant mentioned.*] Am I correctly following how you are evaluating these threats?

Great, we can move on to the next activity. Click the "Finished" button in the upper right.

Advice bucketing [Repeat for each of the 5 parts]
In the next part of this interview, we have some card sorts that focus on specific, proactive advice. As you might know, there are many pieces of advice on the internet about how to stay safer from online hate and harassment. But people have limited time and energy, so it can be hard to know which advice to prioritize.

On the left, you'll see a list of advice we found online for combating [CATEGORY].

We'd like you to bucket each piece of advice into high priority, medium priority, and low priority advice, or advice you don't recommend for a general internet user. Order within the buckets doesn't matter. As before, please talk about your thought process aloud.

Follow-up questions, if not already mentioned by the participant:

- Why did you put this advice in the [high, medium, low] priority box?
- Is there any advice you feel is missing and should be added?

Go ahead and click "Finished" and we'll move on.

Specific advice: top 3
Thanks, you can click "Finished", close this window and stop screensharing now.

Now, all things considered, if you were sitting down with a general internet user, what are the top 3 pieces of advice you would give?

Follow-up questions, if not already mentioned by the participant:

- What makes that the most important?
- To the best of your knowledge, how much has this advice been adopted by general users?

General thoughts
I'm curious who the general internet user is in your mind, while you were thinking about the advice. What kind of characteristics makes for a general internet user?

In your own experiences helping people with online hate and harassment, how do you explain or encourage them to adopt proactive protective practices? (Or do you at all?) When are people most likely to adopt protective practices or seek help? Or if never, what barriers do they experience? When does it make the most sense for people to implement certain pieces of advice?

Are there any online resources or communities for general internet users about hate and harassment that you often recommend?

Follow-up questions, if not already mentioned by the participant:

- What makes them helpful?
- How easy or hard are these resources to discover before an incident occurs? How about during or after an incident? What makes it easier to discover, vs. harder?
- Do you think these resources are comprehensible to a wide audience? What makes them more widely accessible? Should they be?
- In your opinion, what, if any, are the main limitations or gaps with the resources that are currently available?

We've discussed a lot today about what general internet users can or should do to protect themselves from online hate and harassment. How much do you think safety currently falls on individuals right now? In the future, what would make safety less of an individual responsibility?

Wrap-up
Is there anything else you would like to say that we haven't covered?

Do you have any questions for me?

Would you like your name and/or affiliation to be acknowledged in any published material (reports, presentations) that results from this research? We will anonymize all individual responses from this interview (any quotes we share from the research will not be attributed using your name or affiliation).

4 ADVICE GUIDES

We collected 49 online support resources, of which 15 contained advice designed to prevent or mitigate online hate and harassment (versus recovery or coping practices, which we consider out of scope for our study). We list all guides below.

Advice Guide	Author	URL
9 Ways to Dodge Trolls: A Woman's Guide to Digital Security	Safe Spaces	https://medium.com/@securitypositive/9-ways-to-dodge-trolls-a-womans-guide-to-digital-security-701fd3a12d0d
Account Security 101: Passwords, Multifactor, Social Engineering, and You	Crash Override Network	http://www.crashoverridenetwork.com/accountsecurity.html
Assess and Take Action	Online SOS	https://onlinesos.org/action-center/category:identify
Bullying on Social Media	Planned Parenthood	https://www.plannedparenthood.org/learn/teens/bullying-safety-privacy/bullying/bullying-social-media
COACH: Crash Override's Automated Cybersecurity Helper	Crash Override Network	http://www.crashoverridenetwork.com/coach.html
Cyberstalking: Strategies	Take Back The Tech	https://takebackthetech.net/be-safe/cyberstalking-strategies
Data Detox Kit	Tactical Tech	https://datadetoxkit.org/en/home
Dealing with cyberbullying: What would a feminist do?	Guardian	https://www.theguardian.com/commentisfree/audio/2016/may/28/cyberbullying-online-harassment-jessica-valenti-podcast
Deploying Supportive Cyber Communities	PEN America	https://onlineharassmentfieldmanual.pen.org/deploying-supportive-cyber-communities/
Digital First Aid Kit	CiviCERT team	https://digitalfirstaid.org/en/index.html
Distribution of False Information	Online SOS	https://onlinesos.org/resources/action-center/defamation
Distribution of Intimate Images	Online SOS	https://onlinesos.org/resources/action-center/nonconsensualporn
Doxxing	Online SOS	https://onlinesos.org/resources/action-center/doxxing
Doxxing: Tips To Protect Yourself Online & How to Minimize Harm	EFF	https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-how-minimize-harm

Advice Guide	Author	URL
Episode 94: Allying Against Online Harassment with Viktorya Vilk and Emily May	PEN America	https://anchor.fm/penamerica/episodes/Episode-94-Allying-Against-Online-Harassment-with-Viktorya-Vilk-and-Emily-May-ehc6ca
Extortion: Strategies	Take Back The Tech	https://takebackthetech.net/be-safe/extortion-strategies
GCA Cybersecurity Toolkit For Journalists	Global Cyber Alliance	https://gcatoolkit.org/journalists/
Get Help Responding to Online HArassment	Consumer Reports	https://securityplanner.consumerreports.org/tool/get-help-with-online-harassment
Hate Speech: Strategies	Take Back The Tech	https://takebackthetech.net/be-safe/hate-speech-strategies
How to deal with hate speech?	UNIA	https://www.unia.be/en/areas-of-action/media-and-internet/internet/how-to-deal-with-hate-speech
How To Protect Your Data And Remove Personal Information From The Internet For Free	DeleteMe	https://joindeleteme.com/help/diy-free-opt-out-guide/
How to protect yourself from online harassment	Washington Post	https://www.washingtonpost.com/technology/2022/04/25/online-harassment-guide/
How to Shut Stalkers Out of Your Tech	Consumer Reports	https://www.consumerreports.org/digital-security/shut-stalkers-out-of-your-tech-a6642216357/
Into 2020: The State of Online Harassment and Opportunities for Collaboration	Online SOS	https://gallery.mailchimp.com/07817a6d6707692fd4c653d24/files/f730482c-8b79-47d7-99cf-54424b324536/state_of_online_harassment_onlinesos_full_2019.pdf
Mob Harassment	Online SOS	https://onlinesos.org/resources/action-center/mob-harassment
NA: Resource Center	Crash Override Network	http://www.crashoverridenetwork.com/resources.html
OHFM: Further Digital Security Tips	PEN America	https://onlineharassmentfieldmanual.pen.org/further-tips-considerations/
OHFM: Navigating Comments Sections & Message Boards	PEN America	https://onlineharassmentfieldmanual.pen.org/navigating-comments-sections-message-boards/
OHFM: Protecting from Doxing	PEN America	https://onlineharassmentfieldmanual.pen.org/protecting-information-from-doxing/

Advice Guide	Author	URL
OHFM: Protecting from Hacking and Impersonation	PEN America	https://datadetoxkit.org/en/home
OHFM: Protecting Websites	PEN America	https://onlineharassmentfieldmanual.pen.org/protecting-websites/
Online Removal Guide	Cyber Civil Rights Initiative CCRI	https://cybercivilrights.org/online-removal/
Online Sexual Harassment	Online SOS	https://onlinesos.org/resources/action-center/online-sexual-harassment-gendered-threats
Online Threats of Violence	Online SOS	https://onlinesos.org/resources/action-center/online-threats-of-violence
Preventing Doxing	Crash Override Network	https://crashoverridenetwork.tumblr.com/post/108387569412/preventing-doxing
Science in an Age of Scrutiny: How Scientists Can Respond to Criticism and Personal Attacks	Center for Science and Democracy	https://www.ucsusa.org/sites/default/files/2020-09/science-in-an-age-of-scrutiny-2020.pdf
Security Planner	Consumer Reports	https://securityplanner.consumerreports.org/
Self-care: Coping and Healing	Take Back The Tech	https://takebackthetech.net/be-safe/self-care-coping-and-healing
Self-Doxing guide	Access Now Digital Security Helpline	https://guides.accessnow.org/self-doxing.html
So You've Been Doxed: A Guide to Best PRactices	Crash Override Network	https://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices
Something Can Be Done! Guide	Without My Consent	https://withoutmyconsent.org/resources/
Speak Up & Stay Safe(r)	Jaclyn Friedman, Anita Sarkeesian (Feminist Frequency), Renee Bracey Sherman	https://onlinesafety.feministfrequency.com/en/
SSD: Protecting Yourself on Social Networks	EFF	https://ssd.eff.org/en/module/protecting-yourself-social-networks
Talking to Family and Police	Crash Override Network	http://www.crashoverridenetwork.com/familyandpolice.html
Technical Safety Guide	Heartmob	https://iheartmob.org/resources/tech
The Smart Girl's Guide to Privacy: Practical Tips For Staying Safe Online	Violet Blue	https://we.riseup.net/assets/355960/smartgirlsguidetoprivacy.pdf

Advice Guide	Author	URL
Training Curriculum, Gender and Technology Institute	Tactical Tech	https://en.gendersec.train.tacticaltech.org/
What to Do if You're the Target of Online Harassment	Viktorya Vilk for Slate	https://slate.com/technology/2020/06/what-to-do-online-harassment.html
XYZ is a space for practical tools to navigate digital security and privacy from a gender perspective, learn from each other's activism, inspire one another and co-create.	Tactical Tech	https://xyz.informationactivism.org/en/about/

5 COMPLETE ADVICE RANKING

We provide a complete ranking of all advice, ordered by its overall average priority which is the product of both the average priority of the advice (4 = HIGH, 1 = DON'T RECOMMEND) and the average ranking of the threat it is intended to mitigate (7 = TOP THREAT, 1 = LOWEST THREAT).

Advice	Category	Average Threat Ranking	Average Advice Ranking	Overall Average
Mute people who post abusive messages (the person won't know you've muted them)	Toxic Content	5.1	3.8	19.6
Never share your home address publicly	Content Leakage	5.1	3.8	19.3
Use platform-provided tools to automatically filter or moderate abusive messages	Toxic Content	5.1	3.8	19.2
Limit sharing of personal information online generally, being conscious of incidental information leaks	Content Leakage	5.1	3.7	18.8
Block people who post abusive messages (the person may know you've blocked them)	Toxic Content	5.1	3.6	18.6
Encrypt and/or keep intimate imagery offline	Content Leakage	5.1	3.6	18.4
Set restrictive privacy settings on social media (like using a Privacy Check-Up tool)	Content Leakage	5.1	3.6	18.4
Find your personal information or intimate images in search engines or social media to remove or request your data be removed	Content Leakage	5.1	3.6	18.2
Use secure messaging apps for communication	Surveillance	4.7	3.7	17.2
Never share your personal phone number publicly and/or use an alternate phone number (like Google Voice)	Content Leakage	5.1	3.4	17.1
Keep your web camera covered when you aren't using it	Surveillance	4.7	3.6	17.0
Be selective about which online communities you participate in	Toxic Content	5.1	3.3	16.9
Use antivirus software to detect spyware on your devices	Surveillance	4.7	3.5	16.3
Never share location information with apps or in posts or photos, including in photo metadata	Surveillance	4.7	3.4	15.9
Enable any form of 2FA for your most important accounts	Lockout & Control	4.0	3.9	15.7
Disable GPS when not needed to prevent location tracking	Surveillance	4.7	3.3	15.4
Use a strong PIN or passcode for your devices	Lockout & Control	4.0	3.8	15.3
Don't post photos of your activities until after you've left the location	Surveillance	4.7	3.2	15.1
Use an second email address when signing up for websites or creating new accounts	Content Leakage	5.1	2.9	14.6
Be selective about when and to whom you reveal marginalized aspects of your identity	Toxic Content	5.1	2.8	14.5
Use a strong, unique password for all of your accounts	Lockout & Control	4.0	3.6	14.5
Ask friends and family not to share posts or photos about you, and untag yourself in any posts or photos that are shared	Surveillance	4.7	3.1	14.4

Advice	Category	Average Threat Ranking	Average Advice Ranking	Overall Average
Set up alerts to monitor where your name appears in search results (like Google Alerts)	Content Leakage	5.1	2.8	14.0
Use 3rd-party services to help minimize personal information available online	Content Leakage	5.1	2.7	13.8
Periodically delete old social media posts, messages, and emails	Content Leakage	5.1	2.7	13.8
Use a password manager	Lockout & Control	4.0	3.4	13.6
Avoid downloading apps you do not need and remove already downloaded apps that you no longer need	Surveillance	4.7	2.9	13.6
Never send intimate images	Content Leakage	5.1	2.7	13.6
Use a virtual or PO mail box rather than sharing your home address	Surveillance	4.7	2.8	13.2
Don't keep digital copies of your IDs (like a driver's license or passport)	Content Leakage	5.1	2.5	12.7
Do a physical search or digital scan for tracking devices like Airtags or Tiles	Surveillance	4.7	2.6	12.3
Change your passwords regularly	Lockout & Control	4.0	2.9	11.6
Ensure all public records like registered domains or housing records are tied to a pseudonym	Content Leakage	5.1	2.2	11.4
Leave a platform entirely	Toxic Content	5.1	2.2	11.3
Ask friends, family, and colleagues to help keep an eye out for impersonation	Impersonation	3.8	3.0	11.2
Use hardware security keys for your most important accounts	Lockout & Control	4.0	2.5	10.3
Request for your account to be verified (visible indicator of authenticity on platform)	Impersonation	3.8	2.7	9.9
Call your cellular network provider and have a PIN or verbal password associated with your account	Lockout & Control	4.0	2.3	9.4
If a website uses security questions, use a password-like response	Lockout & Control	4.0	2.2	9.1
Use a second, separate SIM card to prevent tracking of your location or phone calls	Surveillance	4.7	1.9	8.9
Reach out to law enforcement in advance to warn about you being a potential target of swatting	False Reporting	3.0	2.3	7.0
Create accounts with your name on all major platforms, even if you don't use all of them	Impersonation	3.8	1.9	7.0
Create a pseudonym or use a different email for each of your online accounts	Lockout & Control	4.0	1.7	6.9
Use a VPN while online to hide your IP address	Overloading	2.3	2.8	6.4
Get DDoS protection for personal websites	Overloading	2.3	2.7	6.2