Building Digital Safety and Meeting our Needs

Insights from Community Leaders:
Activists, Organizers, and Cultural Workers

cyber_bytes

platform

Platform operates across what is currently known as Canada, based on the land known in Kanien'kéha as Tkaronto (Toronto). The land we occupy has been and continues to be home to many Indigenous nations, including the Mississaugas of the Credit, the Anishnabeg, the Chippewa, the Haudenosaunee, and the Wendat peoples, and now hosts diverse First Nations, Inuit and Métis peoples.

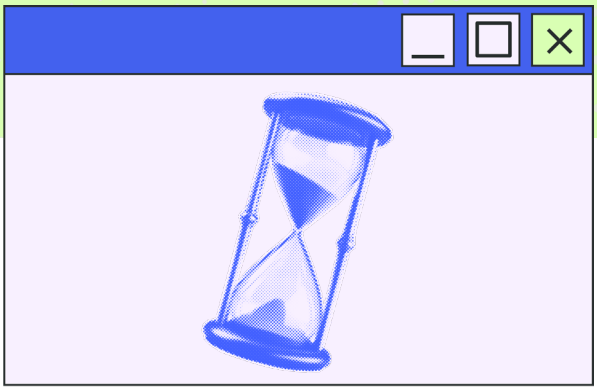
We acknowledge the ongoing colonial violence taking place on this land and its devastating impact on Indigenous communities. The structures that uphold rape culture, sexual violence, and gender-based violence are deeply connected to colonial land-based violence. We are committed to dismantling these power structures through Indigenous-led, anti-oppressive, harm-reduction frameworks, rooted in truth, accountability, and the call for Land Back.

Thank you to all of the community leaders including activists, organizers, and cultural workers who contributed their knowledge, experiences, and time to helping us better understand digital safety challenges, needs, and desires. Thank you to Gachi Issa, Rowa Mohamed, Sarah Tariq, and Sanjit Dhillon for their commitment to the Cyber Bytes project and for their work on this report.

This project was supported by a grant from CIRA's Net Good Program.

net good
BY cira

Summary



Black, Indigenous, and racialized women and 2SLGBTQIA+ activists, organizers, and cultural workers have identified significant gaps in knowledge about digital security and learning opportunities about safety practices that are accessible, practical, and community-centric. While these community leaders have significant concerns about online safety threats, structural barriers prevent them from accessing the information, tools, and safety practices they need to have more confidence in our online security. Women and gender-diverse community leaders need access to more hands-on, accessible learning opportunities reflective of our realities and needs that support implementation of digital safety practices.

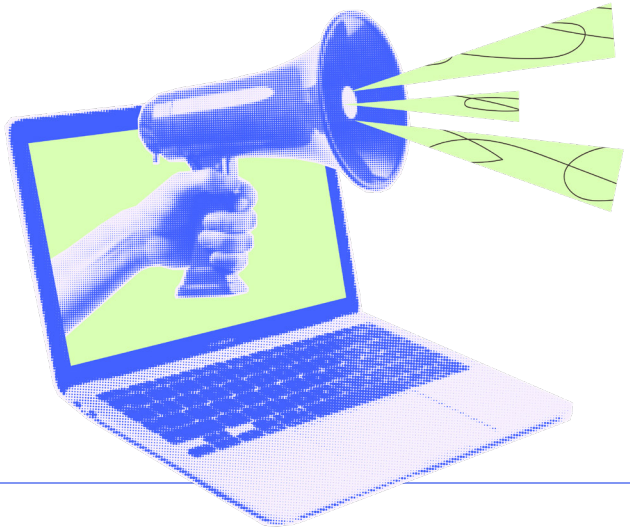
This report provides an overview of online safety concerns, digital security needs, and barriers to access as articulated by women and gender diverse activists, organizers, and cultural workers from predominantly Indigenous, Black and racialized communities. This work draws from 51 survey responses and 15 in-depth interviews. Participants reflect diverse identities and perspectives across cultural backgrounds, gender, sexuality, age, and location:

- 92% of participants are Black, Indigenous, and/or racialized.
- 35% of participants are nonbinary, trans, and/or genderqueer.
- 67% of participants are queer, bisexual, lesbian, or gay.
- 61% of participants are aged 18 to 29; 33% are aged 30 to 39; 6% are aged 40 to 49.
- Responses come from across the country, with the largest clusters in Toronto, Montréal, Vancouver, Hamilton, Ottawa, and Winnipeg.

This assessment reveals a critical demand for enhanced, tailored, and accessible cybersecurity education and resources for community leaders, particularly for activists, organizers, and cultural workers operating in today's complex digital landscape. Educational materials and resources must be developed from an intersectional and trauma-informed lens. The findings illuminate significant knowledge gaps, prevalent safety concerns, and a strong collective desire for practical, community-centric, and ongoing support.

Emerging Insights and Themes

There is a disconnect between the awareness of digital threats and the consistent implementation of proactive digital safety measures. While participants generally understand that online risks exist, this awareness does not consistently translate into robust safety practices due to gaps in knowledge about digital threats and safety practices, a lack of confidence, and other structural barriers.



1

Knowledge Gaps are Fuelling Low Confidence – and Putting Us at Risk

More than half of the participants (55%) shared that they do not feel confident in their digital security knowledge, expressing considerable concerns about potential threats to their online activities. The survey revealed that many participants have not received any cybersecurity training since elementary school, underscoring an outdated and insufficient educational foundation in an ever-evolving threat landscape. The lack of confidence shared by participants is mirrored in practical behaviors: a concerning 60% of respondents admitted to rarely or never changing passwords on important accounts. Only 2% of participants reported using an automatic password renewal manager, though 60% are likely to use a password manager if it's already available on their device. Conversely, 37% do not use a password manager at all, with some using it only for work. When it comes to multi-factor authentication (MFA), 4% of participants reported not knowing what it is, while 60% use it sometimes, and only 35% use it always.

Demands for Foundational Information on Digital Threats and Safety Measures

Participants consistently articulated a strong desire for more accessible and understandable information on fundamental digital security practices. This includes essential topics such as effective password management, safe browsing techniques, and strategies for recognizing and avoiding common online threats, like phishing attempts.

Even among those who are aware of and use tools thought to be more secure, like Signal, there was frequent confusion about how these tools actually protect their data - indicating a need for deeper education on the underlying mechanisms of digital security. Concerns about the privacy of information on communications platforms like WhatsApp and Signal were also expressed.

Critically, most respondents also reported only fundamental or minimal overall technical knowledge of working with computers, highlighting the need to strengthen foundational technology education for youth as new threats emerge.

Significant Urban-Rural Knowledge Disparity

A notable finding was the significant difference in digital security knowledge between urban and rural participants. Specifically, users in urban centers generally exhibited a higher level of awareness, understanding of and confidence in digital safety practices compared to those in more remote or rural areas. This suggests a digital literacy divide that requires targeted educational initiatives to ensure equitable access to critical security knowledge.

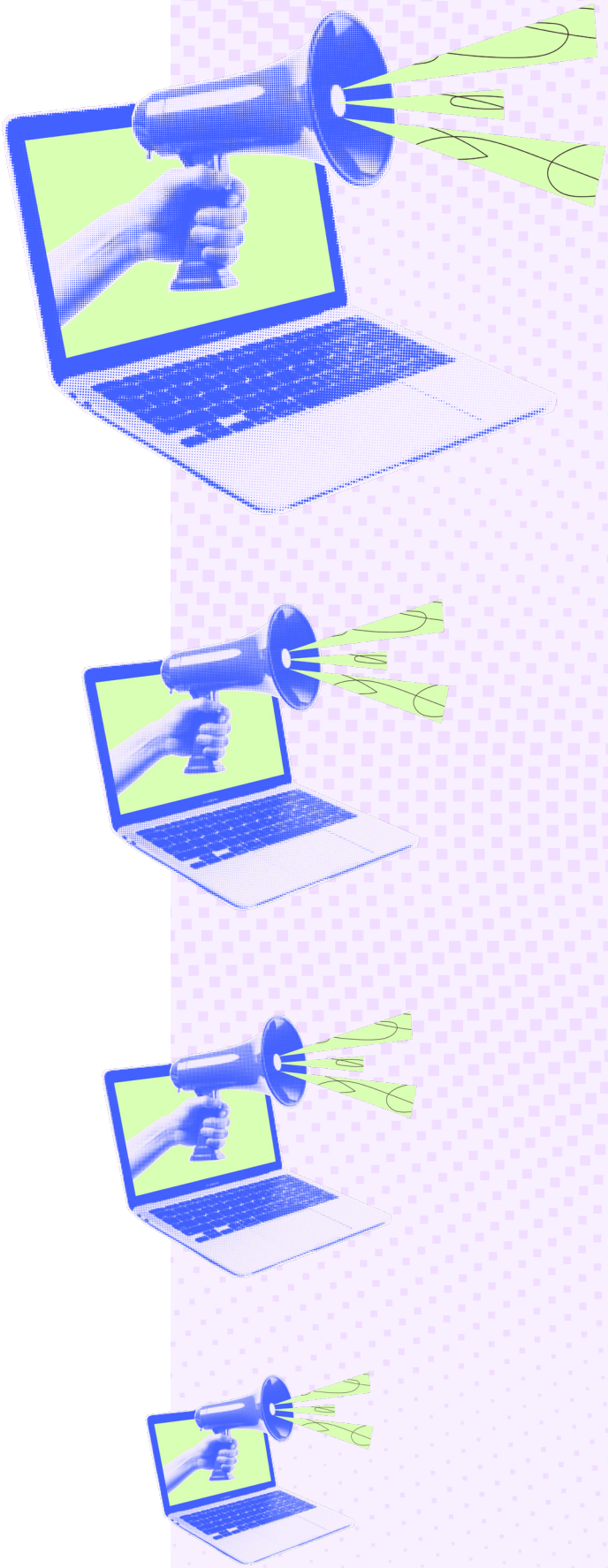
Navigating Legal Implications and Understanding Your Rights

Participants expressed keen interest in understanding the legal implications of their online presence and their rights in digital spaces. There's a demand for actionable advice on what steps to take if you are targeted or doxxed, including legal recourse and reporting mechanisms. Some respondents expressed the lack of seriousness with which police often treat online harassment and death threats, leading to a sense of abandonment and further vulnerability within the community – making "the police" a challenge in themselves.

Information about legal rights and how online presences can be used as evidence against organizers and activists is crucial. This concern extends to how information shared on social media, even in private messages, can be used as evidence against them against activists and organizers that have been unjustly criminalized. There was also an expressed desire to understand how to have media articles and other posts on the internet removed, for example – having an article about someone removed when politically-related criminal charges are dropped.

2

Critical Need for Tailored Training and Learning Opportunities for Organizers and Activists



A resounding call emerged for cybersecurity training specifically designed for activists and organizers, with only 13% of survey respondents having reported taking steps to secure devices for activism and organizing efforts, 11% never doing so, and the rest (more than three-quarters of respondents) only sometimes or rarely. Of the 15 interviewed activists and organizers, 7 (47%) had attended cybersecurity training tailored to activists, and all 15 expressed interest in attending such training if it were available. This highlights a recognition that generic security advice often falls short of addressing the unique operational challenges, threat models, and real-world risks faced by individuals engaged in activism, organizing, and cultural work.

Strategic Social Media Use and Decoupling from Organizing

An interesting observation was the shift in social media usage among activists. While newer activists tend to rely extensively on social media for organizing, more experienced activists (those with 5–20+ years of experience) reported moving away from social media for core organizing efforts, increasingly viewing it as a broadcasting tool rather than a primary mobilizing platform.

Conversely, younger activists (those with only a couple of years of experience) often rely exclusively on social media for their activism. This highlights a need to discuss the strategic use of social media, balancing its effectiveness with safety considerations.

Many survey participants equate social media with civic engagement, creating a challenge when they need to disengage for safety reasons, leading to a feeling of being unable to participate. They want to learn how to use social media for outreach and mobilization without fully revealing personal identity, and how to manage settings to block negative interactions.

33

Deep Dive into Concerns About Online Safety

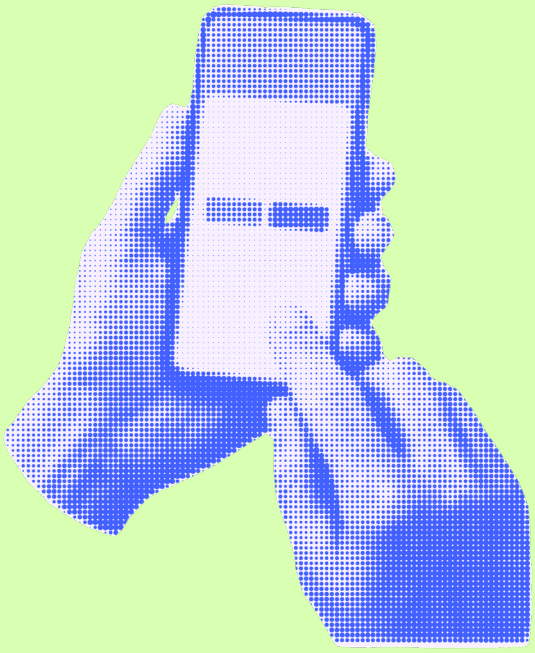
Participants shared anxieties and concerns about online safety that can help us better understand gaps in knowledge, confidence, and existing learning opportunities. These concerns extend far beyond technical vulnerabilities, encompassing profound social and personal dimensions.

Online Harassment, Doxxing and Threats to Physical Safety

Concerns about online harassment and doxxing were overwhelmingly prevalent, with many participants feeling unsafe sharing their identities online due to fear of retaliation, exposure, or for their personal safety.

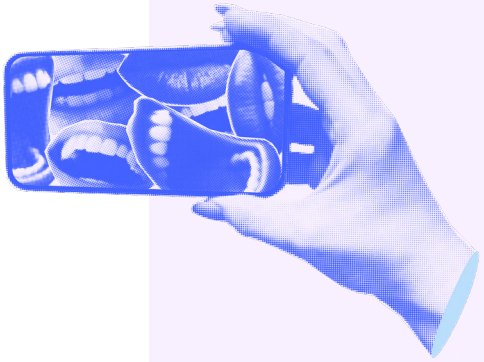
Many respondents expressed fear about how an online presence could affect their physical safety, especially when facing high-stakes situations. This includes instances where digital devices can be seized or scrutinized, such as crossing international borders or navigating interactions with law enforcement.

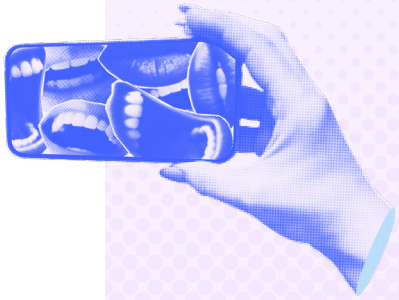
One example cited by a respondent involved water defenders who, unaware of their rights, provided their phone passwords to police during detention. These water defenders were using Slack for organizing, a platform not considered secure for sensitive communications. These findings suggest that there is a critical need for resources that provide activists, organizers, and cultural workers with concrete strategies on how to protect their digital presence and legal rights.



4

The Power of Community Support

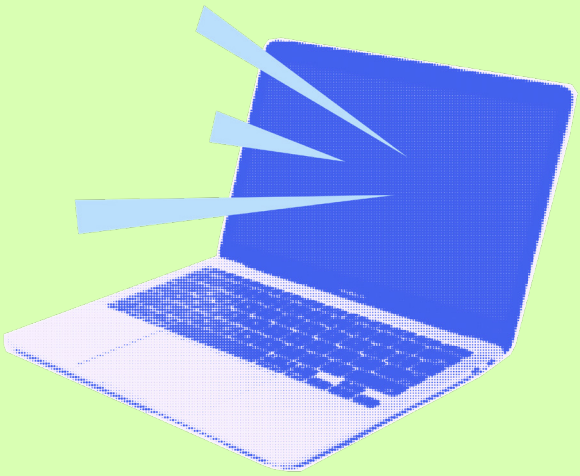




The importance of community support and shared experiences in dealing with online harassment and its associated mental health impacts was emphasized consistently. Participants expressed a clear desire for guidance on creating collective safety plans and fostering supportive networks to navigate these challenges together. Many activists reported experiencing paranoia and changes in their daily habits (e.g., posting location, selfies) due to online harassment, impacting their mental health and how they engaged with their online communities.

Detailed Training and Workshop Needs

Respondents identified the need for practical, relevant, and accessible learning experiences that meet the unique needs of activists, organizers and cultural workers - and particularly those who are women or gender diverse, and/or are Indigenous, Black or from racialized communities.



Demand for Interactive and Hands-On Learning

Participants overwhelmingly called for more interactive and hands-on workshops where they could actively practice using cybersecurity tools in a practical, guided “computer lab”-type setting. This learning-by-doing-approach was seen as crucial for building confidence and retaining knowledge. They want to work on their digital footprints and security measures with direct oversight and instruction. Specific examples and practical activities during workshops are highly desired.

Comprehensive Digital Footprint Management and Secure Communications

Respondents shared significant interest in learning how to effectively manage digital footprints, understanding how algorithms on various platforms influence their online visibility, and gaining practical skills in securing their online communications. This includes detailed information on the implications of using various digital platforms and how to effectively navigate their unique security features. Participants are particularly interested in learning about secure communication tools and their effective use in activism and organizing (e.g. strategies like using timed conversations, and deleting conversations after an action in group chats on platforms like Signal). Respondents shared curiosity in secure e-mail options (e.g. ProtonMail) and would like to better understand cloud security and its intersection with surveillance on different apps.

Accessible and Inclusive Training Materials

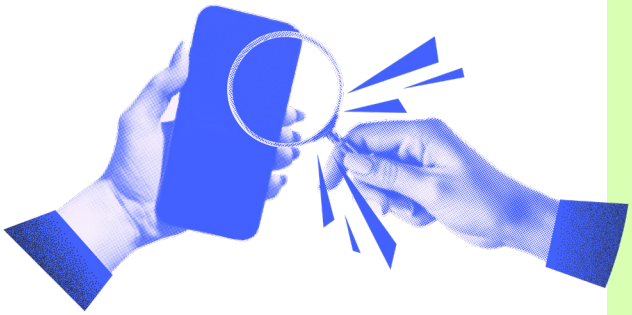
To accommodate diverse learning needs, there is a clear demand for more accessible training materials. This includes the provision of recordings with captions and image descriptions for videos, which would greatly benefit neurodivergent individuals, people with disabilities, and visual learners. Respondents also want training opportunities that are more accessible to rural and remote communities - including widespread promotion when activities are available. Further, cost can be a barrier to many activists, organizers and cultural workers - it is important that training and learning opportunities be free or affordable.

The Need for Racialized Tech Educators

A powerful insight from respondents was the expressed desire for more racialized tech educators to lead training sessions. Some respondents who previously participated in forms of cybersecurity training noted that the training they received was condescending, particularly when delivered by men. This led to disengagement. Having educators who understand the intersection of technology and activism, especially within Indigenous, Black, and racialized contexts, would foster a more inclusive and effective learning environment.

Participants specifically mentioned that facilitators who were "not aligned with their identity or knowledgeable in how to actually relate the information" created reluctance to engage. There is a perceived "falling behind" in tech skills for Indigenous, Black, and racialized individuals in Science, Technology, Engineering, and Mathematics (STEM) and activism, while "fascist tech is evolving," highlighting the urgent need for more racialized tech and digital security teachers who are also organizers.

Cybersecurity trainers should be educated on how marginalized groups engage with content and identify their own biases to avoid "white supremacist mindsets" and approaches in their training.

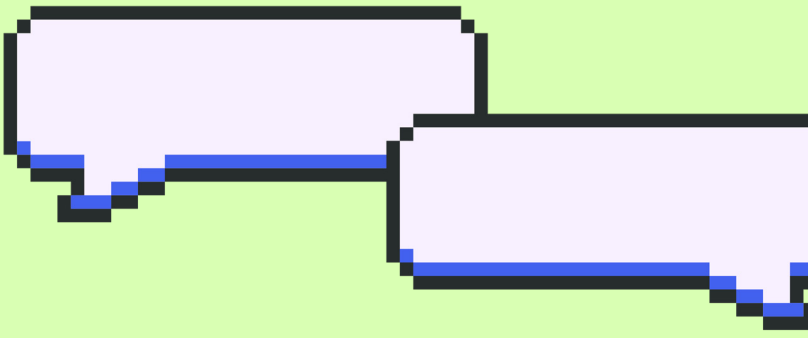


Intersectionality of Risk and Vulnerability

Respondents highlighted that cybersecurity training must explicitly address the intersection of activism, organizing, and digital security, with a strong focus on the unique challenges faced by marginalized communities. This includes Indigenous, Black, and racialized individuals, women, non-binary, gender-diverse people, 2SLGBTQIA+ folks, and those with precarious citizenship status. Participants stressed the importance of understanding specific risks related to their racial, gender, or sexual identity. Respondents shared strong desires for tools and knowledge to conduct individual risk assessments that are sensitive and relevant to these identity-specific vulnerabilities. Marginalized activists, organizers, and cultural workers are also at greater risk of having their work misreported by the media and being criminalized. One interviewee shared that they had been doxxed and later unjustly and irresponsibly identified as a terrorist by a local newspaper. Public criminalization by the media (and others) can have devastating impacts on lives, career prospects, and safety. This type of criminalization, whether through media misreporting or the use of online activities as evidence, is a significant concern for activists and organizers. The potential for online information (including private DMs on social media) to be used as evidence for criminalization was also a prominent concern for respondents.

Addressing Financial Barriers to Secure Tools

Participants articulated significant concerns about the financial barriers to accessing secure tools (e.g. reliable VPNs, paid password managers, etc).This highlights a need for resources that not only explain the benefits of these tools but also provide guidance on choosing trustworthy and affordable options, or exploring community-supported alternatives. Respondents identified that the financial cost of using private and secure platforms that charge fees was a concern and barrier.



Ongoing Support and Resource Requirements

The need for digital security extends beyond one-off training, requiring sustained support and adaptable resources. Participants expressed a strong desire for ongoing support and resources to help them navigate the ever-evolving complexities of digital security in their activism and organizing. This includes continued access to expertise, updated information, and a sense of community - including opportunities for co-learning and knowledge-sharing with other activists and organizers.

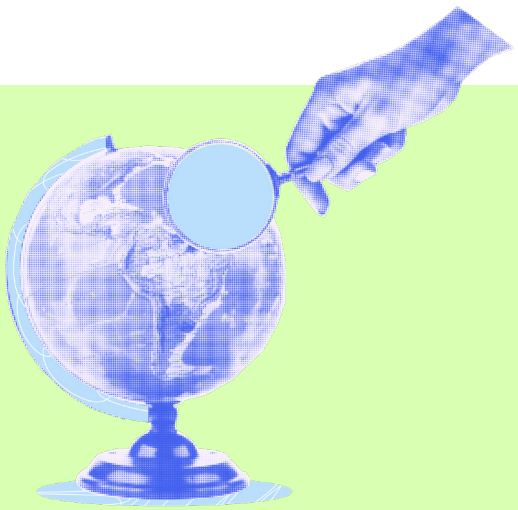
Curriculum Development Insights

This collected data is critical for curriculum development, both in terms of technical information activists and organizers want as well as practical safety strategies they can put in place. Examples of some of the most requested topics include: the security of encrypted messaging applications, specific strategies for protecting privacy while crossing borders (including securing devices and understanding legal rights), discussions on the impact of doxxing and media criminalization on activists' lives, and legal and community support avenues.

Further, respondents identified other topics including how to regain access to hacked accounts, how police scanner boxes work, what employers can track on laptops in use by employees, how to 'scrub' personal information from the internet, filtering social media content, the implications of using different platforms, and the most secure email systems.

Some respondents also identified that they were not aware of accessible resources that compile information and strategies that people can take when gender-based violence intersects with digital safety, signalling a desire to learn further (e.g. domestic violence, cyberstalking, and intimate partner violence).

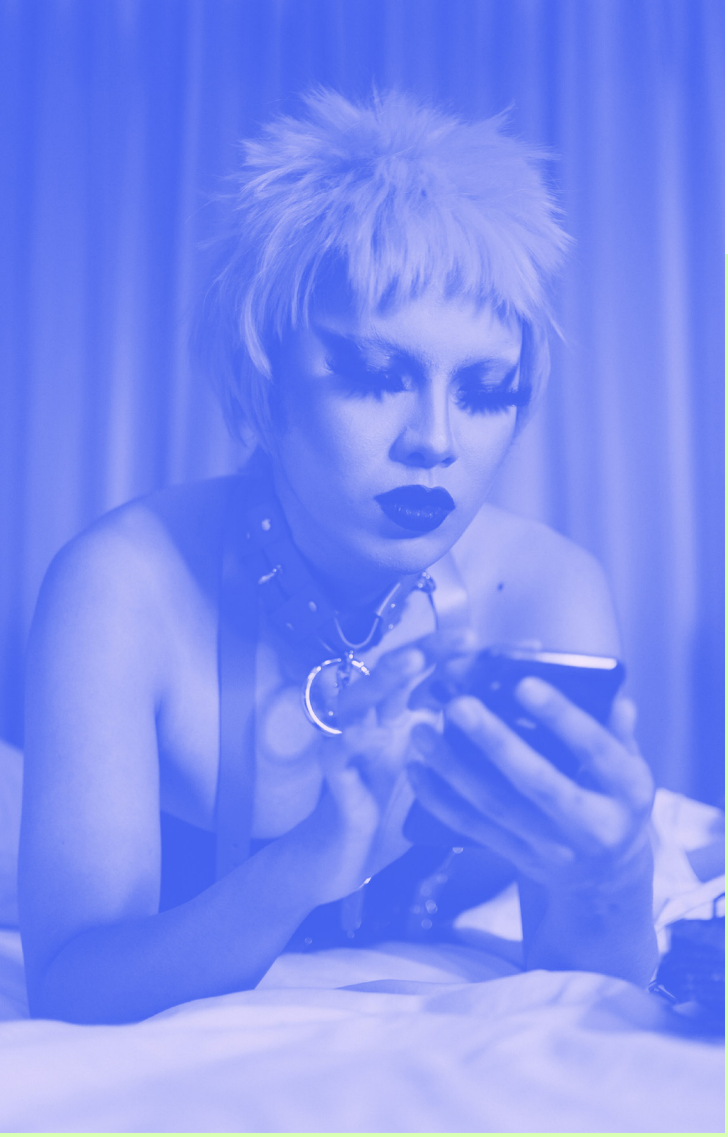
Practical Privacy Measures for Activists - And a Desire to Know More



Respondents identified the need for practical examples and concrete advice for enhancing privacy (e.g. safeguarding personal information by using a professional service address for a registered business to protect personal residential addresses from doxxing).

There are some common measures that respondents noted were somewhat known in their organizing circles: leaving devices at home during actions, using encrypted messaging applications, meeting in person, not taking photos or avoiding capturing identifying features at actions, and having a single designated person for social media/ photography. Still, they were unsure of the effectiveness of these measures, or whether other/better practices should be put in place.

Some respondents also mentioned that they had heard about digital-savvy individuals who had put separate digital systems in place for activism and organizing (e.g. internal servers). There is a significant appetite from organizers and activists to learn about how to 'scrub' personal information from devices and the internet, as well as how employers might have access to information about their organizing activities.



Countering Misinformation Sustainably

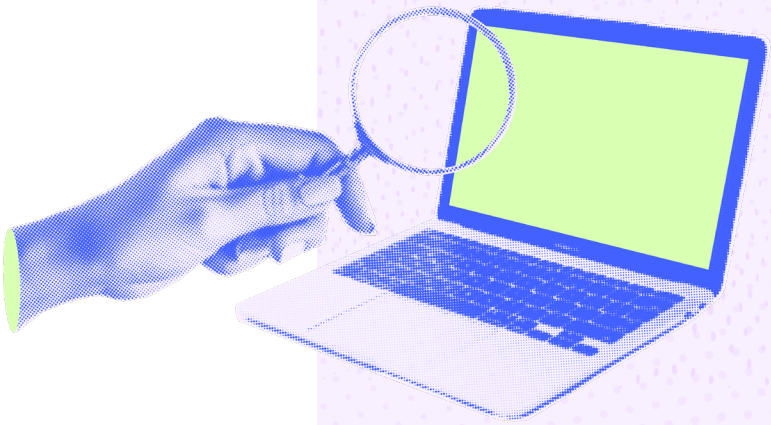
Participants are interested in learning about effective and sustainable methods to counter misinformation in the digital sphere. This work, particularly due to the quantity of misinformation being proliferated online, is extremely demanding on organizers and activists, and learning opportunities and training should include strategies and approaches that help prevent burnout. Some respondents noted that they are actively engaging with misinformation online due to a sense of responsibility to provide visible pushback, and it can come at a significant personal cost. Many respondents shared that they are reluctant to openly share opinions or counteract misinformation due to fear of backlash, harassment, or threats to personal safety.

Focused Resources for Specific Risks

Some respondents identified that they were not aware of accessible resources that compile information and strategies that people can take when gender-based violence intersects with digital safety (e.g. domestic violence, cyberstalking, and intimate partner violence).

6

Challenges Identified in Protecting Digital Privacy and Security



Social Normalization of Openness

A significant challenge is the prevailing social norm of being open and free with personal information online, leading to respondents being dismissed as "paranoid or overly anxious" when practicing cyber safety, or feeling alienated as a result of their reluctance to personally engage or be as present online. Additionally, there's a challenge in effectively explaining to community members why certain digital security measures are necessary (e.g., not taking photos, using secure communication), leading to a lack of broad understanding and consistent adoption. Some participants noted that current training often tells them "what to do" without explaining the "whys."

Lack of Legal Recourse for Online Harassment

A crucial challenge identified is the lack of seriousness with which police treat online harassment and death threats, making it difficult to find effective avenues for redress and support. There is also uncertainty regarding privacy laws that protect individuals online and the challenges of police taking such incidents seriously.

Balancing Security and Accessibility

Social media managers for organizations face a difficult balance between implementing cybersecurity measures and maintaining online accessibility and reach for mobilization and information dissemination. Excluding certain groups and communities becomes a risk if organizing entirely efforts move offline.

Context Collapse and Toxic Online Spaces

Participants are concerned about "context collapse" on social media, where their posts are misunderstood by broader audiences, leading to hate and harassment. Some remain in toxic online spaces for organizing out of a need to counter misinformation, which can significantly contribute to burnout and may not be the most effective form of activism in this space. They are reluctant to share opinions publicly and often resort to "close friends" features to share content.

What Does This Mean?

The data from 52 surveys and 15 interviews reveals that Indigenous, Black, racialized women, 2SLGBTQIA+ activists, organizers, and cultural workers face urgent and intersecting digital security challenges. These gaps are not simply about technical know-how—they are about safety, legal protection, and the ability to continue vital community work without fear of harm or criminalization.

The respondents have made it evident that activists, organizers, and cultural workers are asking for knowledge and practical learning opportunities that centre their needs and communities. They want opportunities to learn and implement digital security practices, while also understanding the “why” so they can feel more confident in their approaches and share them with others in their communities.