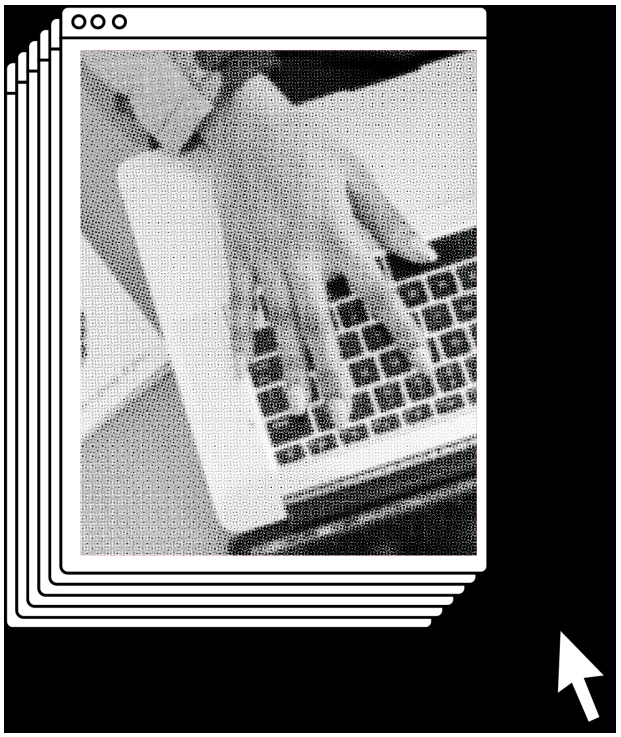
Reconfigure

Feminist Action Research in Cybersecurity



A report co-authored by the Reconfigure Network

Reconfigure Network

The Reconfigure Network is a group of feminist cybersecurity practitioners and researchers who aim to advance industry and academia by using citizen science and action research methods. This report would not exist without the hard work of the following individuals, as well as the contributions of community partners and workshop participants throughout the project. We are forever indebted to everyone's enthusiasm and good-natured collaboration.

This project was also made possible by a UK Research & Innovation Citizen Science Exploration Grant.

	Grant application	Report writing	Workshop organising	Data analysis	Tech support
Julia Slupska	x	x	x	x	x
Scarlet Dawson Duckworth	x	x	x	x	x
Professor Gina Neff	x		x		
Nayana Prakash			x		x
Selina Cho			x	x	x
Linda Ma			x	x	x
Laura Shepherd			x		x
Hayyu Imanda					x
Hubert Au					x
Antonella Perini					x
Romy Minko					x

Table of Contents

Tl;dr

This report presents a 10-month pilot study applying "action research" methods to cybersecurity. The Reconfigure Network ran a series of community workshops in which we invited participants to define their own cybersecurity threats, implement changes to protect themselves, and reflect on the role cybersecurity played in their lives. Our findings can be summarised in five key points:

1. Feelings of avoidance, a lack of awareness, and jargony technical language prevent people from engaging with cybersecurity – our workshops created supportive spaces where participants felt better equipped to overcome these barriers.
2. Our participants demonstrated care and thoughtfulness not only in their own digital privacy practices, but also with respect to the security of their families and communities. This enthusiasm contradicts the stereotype of lazy, uninterested technology users in common cybersecurity narratives.
3. People's digital practices are shaped by privilege and oppression. While advantages like wealth or education help people access knowledge about cybersecurity, experiences of abuse on the basis of gender identity, race, or sexuality both expose people to greater harm and leave them more motivated to take action.
4. Cybersecurity is more effective when it is communal: as our actions affect others (and vice versa), we cannot approach it alone. Setting time aside to discuss online threats and mitigations with members of a community makes it easier and less intimidating to take action.

5. Although such community action is effective, cybersecurity cannot be limited to individuals changing passwords or downloading VPNs. Structural change at the level of culture and legislation is crucial. Such change should realign the incentives of the companies that build digital infrastructures, and is therefore necessary to make the online world safer and more empowering.

Introduction

In today's online spaces where we work, play and coexist, everyone deserves to be safe. This is true now more than ever as the ongoing COVID-19 pandemic and associated lockdowns have confined ever more parts of our lives behind a screen. Over the last seven months, we have seen wave after wave of email-born COVID scams, phishing campaigns, and sophisticated ransomware designed to target remote workers.[1] Online abuse aimed at women, particularly women from Black and minority backgrounds, is also on the rise.[2] Beyond the global health crisis, it seems evident that if everything from banking details, to intimate photographs, to private conversations with friends can be and often is "cyber", then online security should be open and accessible to all.

Yet, mainstream cybersecurity remains far too obscure and intimidating. A clear symptom of this is the exclusion of certain social groups from its research, industry, and mythologies. A significant gender imbalance persists, with only 24% of the global cybersecurity workforce identifying as women.[3] However, representation does not necessarily solve the exclusion problem: a recent UK study found that while they were not underrepresented in the national industry, black employees continue to experience significant discrimination in the workplace.[4] These exclusions and imbalances are illustrated and perpetuated by a well-defined set of stereotypes: cybersecurity is a shadowy realm populated by the (usually white and male) teenage hacker in a hoodie, the nerdy yet brilliant inventor, the socially inept IT guy. They are routinely reinforced on the big screen (see iconic cybersecurity films like War Games or Hackers), TV (see The IT Guys or Mr. Robot) and in the news media.

Cybersecurity elitism can be found in academia just as much as in the industry and media landscape. We see it reflected in the way surrounding research discusses technology users, or the "human factor." Sometimes, users are made invisible or unimportant when research chooses to focus on more powerful actors such as companies, states or the military. The security of ordinary citizens is too often dismissed as a "privacy concern", lying outside the scope of "security" research, which is deemed to be more technical, concrete and serious. On other occasions, users are portrayed as part of the problem. A popular mantra claims that "humans are the weakest link" in cyberdefense strategies.[5] It is the user who chose a weak password, opened the phishing email or shared a nude with the wrong person. While ineffective and sometimes dangerous user behaviours does exist, we must not start by victim-blaming.

---

[1] 'During the Pandemic a Digital Crimewave Has Flooded the Internet', *The Economist*, 2020 <https://www.economist.com/international/2020/08/17/during-the-pandemic-a-digital-crimewave-has-flooded-the-internet>.

[2] Glitch UK, *The Ripple Effect: Covid-19 and the Epidemic of Online Abuse*, 2020 <https://fixtheglitch.org/covid19/>.

[3] (ISC)^2, *(ISC)^2 Cybersecurity Workforce Study: Women in Cybersecurity*, 2019.

[4] NCSC, *Decrypting Diversity: Diversity and Inclusion in Cyber Security*, 2020.

[5] Ciarán McMahon, 'In Defence of the Human Factor', *Frontiers in Psychology*, 11.1390 (2020).

More research should consider the scarcity of learning opportunities for the average person and acknowledge how contradictory, condescending and jargon-ridden existing resources can be.[6]

The Reconfigure project is aligned with an increasingly popular contingent (described in our Related Work section below) that believes a more cyber-aware society can be built *with* users rather than in spite of them. The central question this study aims to answer is "how is cybersecurity different when it starts from ordinary citizens' concerns?" In other words, our work has no rules or signatures for what an individual's cybersecurity should look like.

Cybersecurity research often starts by "threat modelling" —a method in which experts anticipate potential threats to a computer system. We recreated this method without technical jargon, focusing on citizen's experiences of online threats as well as how they relate to cybersecurity both as a concept and a practice. This method generated a variety of novel and unexpected observations. Experiences like creepy targeted advertisements, being profiled online, or harassed using Zoom-bombing fall outside of orthodox cybersecurity concerns but can make people feel unsafe online. Intersecting identities shape individual attitudes: for example, one participant who identified as trans described how online design choices exposed them to the risk of being outed. While harassment on the basis of gender, race or sexuality may make individuals more motivated to learn about online security, participants such as white, university educated men sometimes reported a certain complacency about security as a result of their privilege.

To this end, our report presents the method and findings of a ten-month pilot project applying *action research* methods to the field of cybersecurity. Over the course of these ten months, we ran physical and virtual cybersecurity workshops during which participants were invited to 1) model what they perceived to be security threats, vulnerabilities and priorities in their digital practices, 2) take tangible steps to improve their digital practices during "tech support sessions" —these took the form of self-guided research or acquiring new tools, and 3) share their personal thoughts and feelings on cybersecurity more broadly in an open and non-judgemental group discussion. After the workshops, we held optional one-on-one interviews which gave us a chance to delve more deeply into different topics and explore participants' experiences of the workshops. Our methodology, outlined in the third part of this report, draws on the tenets of participatory action research and feminist theories.At the conclusion of this process, we present a model of citizen participation both to empower people in relation to their digital privacy and to advance the field by incorporating outsider perspectives. Our approach for strengthening digital privacy[7] is predicated on mutual care and inclusiveness rather than condescension and dogma. In this way, we

[6] Elissa M Redmiles and others, 'A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web of California San Diego', *USENIX Security Symposium*, 2020.

[7] The concepts of "cybersecurity" and "digital privacy" are both used to refer to a wide variety of digitally-mediated threats and the defenses against them. Although many scholars and practitioners choose to distinguish between them (see Dourish and Anderson 2006 for a helpful discussion), we use them interchangeably in this report. This is due to a concern that valid concerns about digital security are sometimes dismissed in cybersecurity discussions as merely "privacy problems" (see Slupska 2019 for a discussion.) Furthermore, in workshops and follow up interviews, we asked participants about how and whether they related to these concepts.

reconfigure participation from the passive consumption of cybersecurity information to active engagement. Instead of seeing users, we see citizen scientists.

Related work

Inquiry into "everyday cybersecurity" promotes the understanding of ground-up forms of security instead of assuming expert knowledge is always *correct* knowledge.[8] By doing so, it frames users not as security faults but as assets with agency. As Adams and Sasse put it, "users are not the enemy."[9] As this report is not primarily aimed at academics, we will not provide a comprehensive review of "human-centred security", "usable privacy and security" or "privacy by design" research here. Suffice it to say that exciting work is being done in these communities which does not replicate the implicit hierarchies and assumptions in mainstream cybersecurity research outlined in the introduction.

The Reconfigure project draws on and promotes the work of many activists and advocates in the digital privacy and cybersecurity space. Most notably, we relied on the "DIY Guide to Feminist Cybersecurity"[10] put together by Noah Kelley of the hackblossom collective as the primary resource for our workshops. In addition, we learned a lot from the Tactical Tech Collective's Holistic Security Manual[11] as well as the Electronic Frontier Foundation's Surveillance Self Defence Kit[12]. All these resources share a commitment to spreading cybersecurity awareness and skills in an accessible way. Lastly, although we did not come across them in time to promote their resources in our workshops, we want to highlight the important work of Seyi Akiwowo and Glitch UK[13], who are combatting online abuse promoting digital self-care[14] and digital citizenship[15].

As part of this lively corner of the cybersecurity world, we share our fellow activists' commitment to directly improving citizen empowerment in matters of online safety. We consider that our unique contribution is to combine digital privacy workshops with citizen science and action research —a methodology outlined below.

Methods

[8] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude P. R. Heath, 'Too Much Information: Questioning Security in a Post-Digital Society', 2020 <https://doi.org/10.1145/3313831.3376214>; Lizzie Coles-Kemp, Debi Ashenden, and Kieron O'Hara, 'Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen', *Politics and Governance*, 2018 <https://doi.org/10.17645/pag.v6i2.1333>.

[9] Anne Adams and Martina Angela Sasse, 'Users Are Not The Enemy', *Communications of the ACM*, 1999 <https://doi.org/10.1145/322796.322806>.

[10] https://hackblossom.org/cybersecurity/
[11] https://holistic-security.tacticaltech.org/
[12] https://ssd.eff.org/en
[13] https://fixtheglitch.org/digital-citizenship/digital-citizenship-our-definition/
[14] https://fixtheglitch.org/digitalselfcare/
[15] https://fixtheglitch.org/digital-citizenship/digital-citizenship-our-definition/

There are a variety of participatory approaches to action research, in which researchers and participants work together to address a problem and learn from the shared process.[16] "Citizen science" is a related form of research conducted, in whole or in part, by amateur (or nonprofessional) scientists.[17]

Action research: a form of research in which researchers and participants work together to address a problem and learn from this attempt in cycles of "action" and "reflection"

Action research stems from the belief that all people affected by an issue should be involved in the processes of research inquiry.[18] Its methods are democratic and collaborative, seeking to build knowledge *with* rather than *about* participants. In particular, intersectional feminist forms of action research seek to expose the power relations that lurk under the trappings of expertise through research methods which empower participants.[19]

Following this tradition, we designed workshops as self-contained bubbles within participants' lives, which intervened by providing a space for improving their digital privacy practices and reflecting on surrounding issues. Our workshops invited "ordinary", or "inexperienced" individuals to actively shape understandings of cybersecurity, precisely because we consider no individual to be truly ordinary or inexperienced. Our recruitment methods —fliers, social media, and community newsletters— emphasised that participants did not need any expertise to contribute. Because we recruited locally and through our own networks, samples should not be taken to be representative of the broader population. Nonetheless, our participants all had valuable insights based on their experiences of online life.

Although there is no one unified "feminism", feminist theories and methods often pay close attention to care, emotionality and personal "standpoint", in addition to a strong emphasis on collaboration.[20] We aimed to create an environment of mutual care and

[16] Sarah Kindon, Rachel Pain, and Mike Kesby, 'Participatory Action Research: Origins, Approaches and Methods', in *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*, 2007.

[17] M V Eitzel and others, 'Citizen Science Terminology Matters: Exploring Key Terms', *Citizen Science: Theory and Practice*, 2017 <https://doi.org/10.5334/cstp.96>.

[18] Stephen Kemmis, Robin McTaggart, and Rhonda Nixon, *The Action Research Planner: Doing Critical Participatory Action Research*, *The Action Research Planner: Doing Critical Participatory Action Research*, 2014 <https://doi.org/10.1007/978-981-4560-67-2>; Kindon, Pain, and Kesby.

[19] Sasha Costanza-Chock, 'Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice', in *DRS2018: Catalyst*, 2018 <https://doi.org/10.21606/drs.2018.679>.

[20] Please note that these texts are indicative but not an exhaustive summaru of feminist research on standpoint epistemology: Patricia Hill Collins, *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment* (Routledge, 1990) <https://doi.org/10.2307/2074808>; Sandra Harding, 'Feminist Standpoint Epistemology', *The Gender and Science Reader*, 2001; Donna Haraway, 'Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective', *Feminist Studies*, 1988 <https://doi.org/10.2307/3178066>.

support, with the tech support team set in a particular position of taking care of others' needs. Our questions focused on emotionality and personal experience —topics in which anyone's and everyone's answers would be valid. Furthermore, at the start of each workshop and in the section on "Our Standpoint" below, we shared our personal experiences and how they shaped our views of security.

Each workshop followed a similar format:

1. an introduction welcoming participants and outlining our motivations and goals

2. a brief questionnaire on demographics, as well as an opportunity for participant introductions and reasons for attending the workshop

3. a "threat modelling" session focusing on what participants wanted to protect in their online life, broken down into three questions:

    - Which parts of your digital presence are the most important to you to protect?
    - What makes you feel threatened online? Can you remember the last time you felt unsafe?
    - Which parts of your digital security would you like to improve?

4. a "tech support" session in which we pointed participants to online resources and worked with them to make practical changes and improve understanding
5. a general discussion on the nature of and future directions for cybersecurity, using the following questions:

    - How does cybersecurity make you feel?
    - How do personal experiences (such as gender, race, class, educational background, anything else) shape your engagement with cybersecurity?
    - Are there any cybersecurity tools that you haven't encountered yet but that you wish existed?
    - Should "good cybersecurity citizens" keep up to date with cybersecurity practices (such as those in the DIY Handbook)?

Because we did not collaborate with participants on the design of this methodology, our study cannot be considered fully participatory. In other words, our results lean more heavily on our (the authors') own motivations and assumptions than if they had emerged from a "true" PAR framework. However, we often partnered with community organisations which were either recruited through our own network or reached out to us proactively(discussed further in the section on *Special Workshops*). Different aspects of the workshops —such as discussion questions and tech support— were tailored to reflect our partners' needs.

Threat modelling: a cybersecurity method which systematically models "assets" (i.e what you want to protect), "threats" (i.e. how you could be attacked & potential attackers), and "mitigations" (what you can do to defend yourself).

The practice of cybersecurity "threat modelling" usually relies on technical experts to identify potential threats, vulnerabilities, and how to mitigate them. Despite being presented as abstract and impartial, this process often relies on previous assumptions about everyday users. Feminist standpoint theories advocate for the use of women's experiences as an alternative lens for social science research.[21] In contrast, conventional cybersecurity threat modelling methodologies deploy what Haraway dubs the "god trick of seeing from nowhere", positioning the researcher's imagination of possible threat scenarios as an abstract threat model.[22] This results in research and policy which omits many forms of technological abuse: for example, a study conducted by one of the authors of this report found that most smart home threat models focus on remote hackers or thieves and do not anticipate that a current or former partner could be a threat.[23]

Standpoint theory: a feminist theoretical perspective according to which knowledge stems from your social, personal and political experiences. In societies stratified by gender, race, class and other categories, your social position shapes what you know.

Rather than dictating what threats citizens *should* be worrying about, this project develops a model for eliciting and listening to citizens' concerns to expand the scope of threat modelling in cybersecurity. This is threat modelling for humans rather than systems. Participant answers in this initial discussion would guide which areas they focused on in the hands-on part of the workshop aided by tech support (see the *Tech Support Guidelines*).

Tech Support Guidelines

We aim to create a safe, open, and social space where participants and tech support help each other learn and improve their digital privacy practices. We want to move away from stereotypical tech support based on shaming people for bad practices and dictating digital privacy "do's and don'ts". To this end, we ask anyone playing a tech support role at Reconfigure workshops to:

1. Take *care* of your participants: be *attentive* to their needs and personal experiences, do not assume that what works for your digital privacy practices will work for theirs. Note down participant answers during the first discussion section (esp. "What aspects of your digital security do you wish to improve?") and use these as starting points in the Tech Support Session.

[21] Sharlene Hesse-Biber, Patricia Leavy, and Abigail Brooks, 'Feminist Standpoint Epistemology: Building Knowledge and Empowerment Through Women's Lived Experience', in *Feminist Research Practice*, 2012 <https://doi.org/10.4135/9781412984270.n3>.

[22] Haraway.

[23] Julia Slupska, 'Safe at Home: Towards a Feminist Critique of Cybersecurity', *St Antony's International Review*, 2019.

2. Avoid *techsplaining* and *mansplaining,* understood as forms of explaining where the goal is to show off your knowledge rather than responding to the participant's needs.

3. Be honest with your *limitations*: we are not certified or professional security trainers and we are not here to be heroes or rescue anyone. **If any participants describe a situation in which they or someone they know is in danger, make sure to suggest they contact the police, domestic violence services (such as Women's Aid[24] or a local service such as OSARCC[25]), or the National Stalking Helpline[26].**

4. *Enjoy yourself*: helping someone set up PGP or reading through Tor troubleshooting can be surprisingly fun. If someone asks a question you don't know the answer to, stay transparent and enthusiastic: "Good question! I don't know the answer. Do you want to Google it together?

All formalised questions were asked using Mentimeter, an interactive online platform. In both the recruitment materials and introduction, we explained to participants that taking part in the "research" aspect of the project was entirely optional, and that they could participate in the discussions, tech support and snacks without formally *contributing data*. If they wanted to share their thoughts and stories, they could do so anonymously on their own devices through the Mentimeter platform, in which case their contributions would be projected on screen in real time. Alternatively, participants could opt-in to recorded focus groups with the same questions. The ability to opt in and out at will was important to the creation of safe spaces around sensitive discussion topics. Ultimately, 419 individual Mentimeter responses and 4 focus groups across 7 workshops. Follow-up interviews with 7 workshop participants explored their contributions in further depth.

Using proprietary technologies can pose ethical and pragmatic challenges for researchers. For example, in our workshops with Power Play/Victims of Image Based Abuse, we were not able to use Mentimeter as we discovered too late that their subscription policy had changed. This meant we were not able to provide participants with the flexibility to opt out of data collection, in a setting where it would have been particularly valuable given the sensitive nature of the workshop. We mitigated this by recording a focus group and giving participants a chance to amend or withdraw comments.

An important strength of the action research methodology is an iterative cycle of action and reflection.[27] By developing our own format for collecting participant views and trying to build a supportive environment, we saw first-hand the challenges and opportunities of bringing agency and empowerment to people's digital lives. Our follow up interviews also allowed us to engage with direct feedback about the

[24] https://www.womensaid.org.uk/
[25] https://www.osarcc.org.uk/
[26] https://www.suzylamplugh.org/pages/category/national-stalking-helpline
[27] Kindon, Pain, and Kesby; Kemmis, McTaggart, and Nixon.

workshops, —what worked and what didn't— as a form of "participant-centred reflexivity" (i.e. reflexivity which comes from participants rather than a researcher's reflections on their own study).[28]

Reflexivity: a practice in which you reflect on how your own experiences, beliefs, and standpoint in the world shape your research

Data was analysed using thematic analysis[29]: following an initial coding of the first workshop, a codebook with 18 "topics" and 29 "themes" was used for all Mentimeter responses, focus group transcripts, and interview transcripts (please find the codebook in *Appendix 1*). Each document was coded by two researchers separately, who then discussed any disagreements and settled on final codes. 5 topics and 8 themes which were not noted in the initial analysis emerged in this process.

Limitations to this project include fairly small sample sizes for the questionnaire and interviews in comparison to conventional surveys or interview methods: approximately 10-12 participants in each of the eight workshops (or a total of around 90 participants).[30] Furthermore, the environment we create could be criticised as leading on account of our explicitly feminist approach, which we signalled to participants before and during the workshops. Thus, our recruitment materials likely attracted a self-selection of participants who would identify as feminist, or at least who would not be put off by that label. That being said, these methods reflect the theoretical commitments of the project, which see research as a form of intervention rather than a neutral data-collection exercise. The workshops were designed to be a place where we could co-create knowledge with our participants: for example, sharing participant responses on a screen throughout the workshop allowed participants to comment and react to the contributions of others, creating a sense of communal sharing and debate.

Our Standpoint

Much of the initial motivation for this project came from the shared experiences of the two co-founders of Reconfigure and co-authors of this report: Scarlet Dawson Duckworth & Julia Slupska. We share an academic background in political theory and social science, and we both entered the field of cybersecurity between 2017 and 2019. Julia is now a PhD student at the Centre for Doctoral Training in Cybersecurity at the University of Oxford, and Scarlet works as a Cyber Technology Expert for Darktrace, a cybersecurity AI company (and partner of this project). While we were both excited to learn, we also noticed a few shortcomings in our newfound field. We would often find ourselves commiserating over the lack of mainstream research on tech-enabled gendered violence, or sexist comments overheard at security conventions and in the classroom, ranging from condescension to outright hostility towards women and those from non-technical backgrounds. This and our desire to improve our own digital

[28] Kathleen Riach, 'Exploring Participant-Centred Reflexivity in the Research Interview', *Sociology*, 2009, 356–70 <https://doi.org/10.1177/0038038508101170>.

[29] Virginia Braun and others, 'Thematic Analysis', in *Handbook of Research Methods in Health Social Sciences*, 2019 <https://doi.org/10.1007/978-981-10-5251-4_103>.

[30] Although participants were welcome to join multiple workshops, we did not observe instances of this occurring.

practices lead to the idea of creating a collaborative, safe space where people could troubleshoot, discuss and educate themselves together.

We shared our backgrounds and the way they motivated the project at the start of each workshop a form of "reflexivity."It is likely that hearing about our experiences influenced participant's beliefs about cybersecurity, including how it is shaped by gender or barriers to entry. However, we instinctively focused on aspects of our identities—being women from non-technical backgrounds—which were treated in various subtle ways as disadvantages in the context of cybersecurity. It is important to note that this form of (incomplete) reflexivity can obscure all the privileges that also influence our work: we are both White, cis-gendered, able-bodied and graduates of an elite academic institution that is inseparable from a colonial history. As a result, the ways in which cybersecurity reinforces other forms of oppression like race, class and disability, are not immediately obvious to us. We found feminist theories and methods particularly useful both for making sense of our own experiences and as a framework for the kind of cybersecurity research and practices we would like to see in the world. A project which centred critical race, disability, or anarchist theory might have shared some of our assumptions but would likely have asked different questions, resulting in different findings.

Covid-19 Adjustments

As a result of the COVID-19 pandemic and related lockdown measures, several workshops were postponed, and the remainder were moved to an online format using the same survey software (Mentimeter) and the video-conferencing platform Jitsi.[31] We initially viewed this as a serious setback, as we found it harder to recruit participants and more awkward to provide tech support without being in the same room. Furthermore, conducting workshops online leaves the study more vulnerable to technical malfunctions.

However, in the later stages of both the lockdown and this project, we started to see the benefits of the online format. As workshops already required participants to bring laptops or smartphones to access websites such as Mentimeter and the DIY Guide, we were well positioned to develop online content. Furthermore, participants seemed to find it easier to focus on the DIY Guide and tended to implement more concrete actions compared with a physical group setting. The move online also increased accessibility of the workshops to more international locations or to people unable to travel due to disability or financial constraints. Lastly, Mentimeter's interactive features helped create a sense of collaboration and togetherness despite participants being far apart and going through a difficult time.

Ethics

[31] Jitsi was chosen due to enhanced security features such as personal servers which allows for customised protection that is equivalent to an E2E encryption. It has been widely endorsed by privacy advocates such as Edward Snowden and the developers of the Tor project (see Ivan Mehta, 'A Look at How Jitsi Became a "Secure" Open-Source Alternative to Zoom', *The Next Web*, 2020 <https://thenextweb.com/apps/2020/05/21/a-look-at-how-jitsi-became-a-secure-open-source-alternative-to-zoom/>.)

Ethical concerns for this study included the risk that participants may not feel comfortable discussing certain workshop topics. This was particularly true for those participants who had experienced sexual abuse and other identity-based attacks online. We addressed this by reminding participants that each question is optional and giving them multiple contribution opportunities and fora to choose from, including the questionnaire, group discussion and one-on-one interviews. For workshops focused on sensitive topics, we also allocated special breaks for self-care and designated an organiser that participants could speak to if they were feeling distressed. Furthermore, there are risks inherent to public events, such as harassment or trolling. We are pleased to report that these complications did not arise at our workshops as far as we are aware. However, we prepared strategies for dealing with such situations in collaboration with our tech support team.

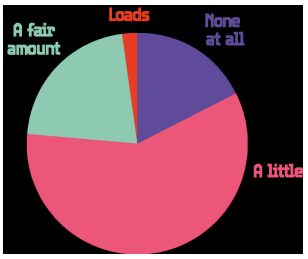
Findings

At the beginning of each workshop, we asked participants a set of demographic questions including gender, age, and knowledge of digital privacy. This was an opportunity to get a sense of the room and begin to create a welcoming space for all groups, especially those underrepresented in cybersecurity and digital privacy discussions. The results presented below are not an exhaustive depiction of the workshops in practice, as participants were free to pick and choose which questions they wanted to answer (although approximately 90 participants attended the workshops in total, many of them chose not to answer certain questions, and some did not contribute at all).

We note that we did not collect demographic data on race and ethnicity until the final three workshops, and did not collect data on class and education level. We view this as a significant oversight, as racial, class and educational disparities are ingrained in cybersecurity culture and equally important to address. Furthermore, it is possible that this omission unintentionally signalled to our participants that we were not as interested in this aspect of their identity, therefore shaping the data we collected.

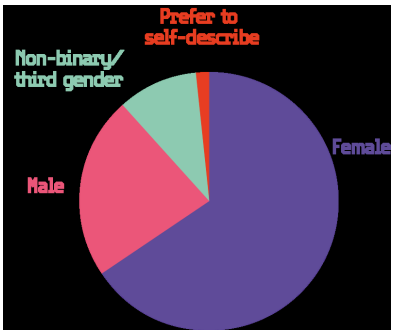
How much digital privacy/cybersecurity knowledge do you have?

None at all	9
A little	30
A fair amount	11
Loads	1
Total	51



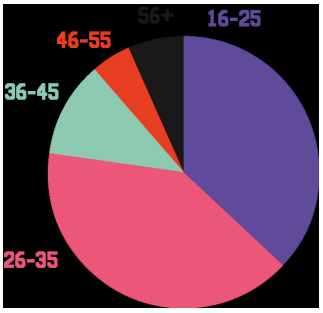
Which gender do you identify as?

Female	40
Male	14
Non-binary/third gender	6
Prefer to self-describe	1
Total	61



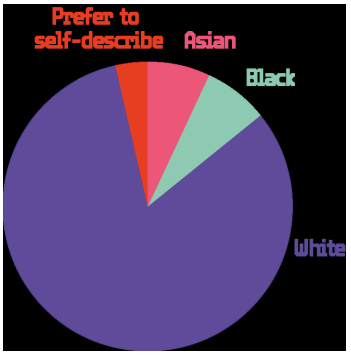
How old are you?

16-25	23
26-35	25
36-45	7
46-55	3
56+	4
Total	61



How would you describe your race or ethnicity?

Arab	0
Asian	2
Black	2
White	23
Prefer to self-describe	1
Total	28



Threat Modelling

As mentioned in the methods section, cybersecurity design often starts systematically modeling "assets", "threats", and "mitigations". Rather than teaching this formal system and its terminology, we started each workshop with participant's own reflections on parts of their online life that they value, what makes them feel threatened online, and which security practices they would like to improve. These questions intentionally did not use the words "cybersecurity" or "digital privacy" in order to avoid restricting definitions.

Throughout the findings section, you will find call-out boxes in the side-bar which display verbatim responses that participants chose to post through our Mentimeter platform. These were chosen both to highlight common responses and to showcase comments which were interesting or delightful.

Which parts of your digital presence are the most important to you to protect?

- Financial details and personal information
- data others post about me
- Information related to protected characteristics that appears to be 'scraped' from multiple sources
- Work with children, wanting to keep private/activism life away from children and families,
- Everything!!!
- Privacy when doing online activism
- My day-to-day activity, my personal image (i.e. likeness), my deepest fears and anxieties
- Location data
- I'd rather have my bank accounts emptied than all my private messages aired and shared

This question invited participants to reflect on their digital selves and associated priorities. In dryer terms, we wanted participants to identify their "assets". Private messaging was the most frequently mentioned asset, followed by financial data. The security of private messages (often relating to social media platforms) connects with recurring concerns about exposure of the digital self and intimate data types. Participants frequently highlighted the vulnerability of their personal information —information that could help paint a picture of who a person is, or reveal private interests, relationships or political alignments. Thus, we observed that anonymity, reputation and intimacy were also among the most frequent themes, reflected in comments such as "being stalked by strangers or friends of friends and finding boundaries between being polite and being safe", and "compromising or embarrassing details can just be spread around the world or amongst a person's whole contact group".

Despite financial data's popularity when modelling assets, it was only rarely mentioned in the tech support and discussion parts of the workshops. It is possible that finances and banking initially sprang to the minds of participants when thinking about assets, because the consequences of having bank details stolen are easy to conceptualise (and highly mediatised). However, the absence of this topic from the rest of the workshops

suggests that it was not as close to participants' hearts as "being able to have privacy over your own intimate space", for instance. During the tech support sessions, many chose to focus on social media, messaging platforms and emails, and discussions often raised more intimate themes. For example, one participant noted that: "I would say, I'm more worried about being socially shamed, publicly shamed, than someone stealing my money."

Responses were sometimes specific ("Health tracking and search history"), and sometimes less so ("The permanence of my digital footprint"). The theme of knowledge was prevalent, suggesting that some participants felt they were not fully cognizant of what their "crown jewels" should be: "there are many facets of my digital presence I don't know about".However, expressions of uncertainty were far outnumbered by impressively concise responses listing such assets as "photos", "location data", "facial recognition" and even "biometric targeted ads". This demonstrates that when prompted, many participants were able to conceptualise their digital footprints and identify their priorities with some precision.

Many responses referred to the idea of online tracking and data harvesting, often expressing the desire not only for more control (the most frequent theme for this question) but also more clarity over what data is being collected and, crucially, who is doing the collecting. One participant wrote: "I want to know who is looking, more than what they are looking at". This relates to an illuminating nuance within participants' privacy needs. While many would like to restrict or decrease the amount of personal data that is available online, it seems equally if not more important to understand and selectively manage who that data is available to. According to one participant, "just having controls over what goes to whom is massive. If you're willing to share with one person, it doesn't necessarily mean you're willing to share the same thing with anyone else". Being secure online often starts with being able to know and choose who can see what with confidence.

What makes you feel threatened online, can you remember a specific time you felt unsafe?

- The presence of my Chinese aunties online is pretty terrifying
- Being followed by bots on Twitter
- Directly threats on twitter messaging from weirdo stalkers
- Times when you challenge something, racism etc and then lots of people will defend the situation or say it never existed/happened/shouldn't be discussed. You get bombarded and worried it can lead to doxxing.
- My personal experiences of lack of safety online have always been minute interactions with someone I know, often with a flirtatious communication edging into uncomfortable territory.
- Zoom meeting was hacked by immature boys in masks showing silly things they thought were disturbing. My data being shared on zoom with facebook and google by zoom.
- People monitoring online shopping

Private messaging continued to be the most popular topic, followed by anonymity and online tracking. A great deal of emphasis was placed on data, from "personal data", to

"financial data", to "biometric data". Some participant concerns about their data were more specific ("employers accessing old data"), and others reiterate a desire for further knowledge of an ill-defined danger ("not knowing who knows what about me and my personal information"). In fact, participants' perceived lack of knowledge was sometimes framed as a threat itself: "Realising my own naivety in how 'safe' I normally feel". While this may reflect cybersecurity's exaggerated emphasis on user responsibility, it also highlights the importance of building self-confidence through learning and practice.
Participants often mentioned targeted advertising when asked what made them feel threatened online. While rarely treated as an "attack" in conventional cybersecurity literature, targeted advertising does offer a rare glimpse at the extent to which third parties access and utilise our data. It also provides an interesting hypothetical: what would cybersecurity look like if it defended users against threats like targeted advertising?

Although the theme of self-doubt was present, participants also expressed a lack of trust in external entities such as governments, companies and other users. Participants felt threatened by corporate activities related to "data gathering" or "targeted ads". One participant who self-described as an immigrant mentioned a "fear of private conversations being used in some way, shape or form to make decisions that materially affect my security [in this country]". Overwhelmingly, many responses drew attention to threats from peers such as "online harassment", "trolling", and "doxxing". Survivors of image-based sexual abuse faced a particularly challenging set of threats. Not only had they experienced ex-partners sharing intimate images —including videos filmed without their consent— online, they also described ongoing harassment on social media as strangers continuously re-shared links to pornography sites which which refused to take down these images and videos Hacking was also brought up occasionally, but overall very few responses mentioned "mainstream" security threats such as viruses or malware.

Finally, several participants offered critical reflections on the word "threatened". Many replied that they did not often feel threatened ("nothing makes me feel particularly threatened online"), or that they would use a different word ("Threatened is too strong- annoying if you are not sure about a phishing mail"). The common thread here could be thought of as a sense of safety in everyday internet and technology use, with moments of fear or anxiety triggered only by direct experiences of attack, or otherwise unsettling experiences such as unsolicited messages or targeted advertising.

Which parts of your digital security would you like to improve?

- Secure communication channels/knowing what makes them secure
- i know that not everything can be covered in 1 workshop so where should i be going to learn after this workshop - i dont know where to get good information
- Data (personal, public). Taking care of online events and the safety of participants.
- How to prevent data being used by adtech
- cloud storage, password security
- Virus protection and how to know when my computer has a virus. How to protect against zoom bombing and is zoom the most ethical and secure platform to use?

With this final threat modelling question, we wanted participants to set their own expectations and goals for the workshop, leading directly into the practical "tech support" sessions. Responses presented an interesting spread of intentions related to knowing ("finding out unknown unknowns"), and doing ("getting out of random websites i signed up for in the past"). Some felt unable to comment in detail: "Probably lots, but difficult for me to answer when I don't understand fully how digital security works". Others articulated this as an explicit intention to seek out and build knowledge. "Improvement" was equated with "tracking", "identify", "knowing", "finding out", "awareness". One participant wanted to "identify where my data is and what it is", another to "understand as clearly and concisely as possible how my data is being used".

Alongside information-gathering goals, we also collected some clearly defined action goals. Participants wanted to "secure", "change", "download", "share", "delete". The most common topic here was password, which perhaps seemed accessible and instuitive as a first step. Private messages and online tracking were also popular topics. The desire to "disentangle" oneself from technology was persistently alluded to, with some participants wishing to "get out of random websites", or "more effectively extract" themselves from social media. Interestingly, interviewees were likely to use this question as an opportunity to reflect on the different obstacles they faced with making concrete improvements. Their workshop experience and plans for their digital security in the future were caveated with thoughts on lack of time, motivation and other reasons for avoidance. These and other barriers to inclusion in cybersecurity will be addressed further in our section on reflections and limitations.

Discussion

How does cybersecurity make you feel?

- Exhausted
- More aware about what I can do
- Ignorant
- Overwhelmed - learned a lot - but still thinking what is too much
- Initially - stupid. Then - frustrated. Later - smug... or a failure depending on the outcome. After - paranoid.
- Frustrated
- nostalgic - passwords reflect different parts of my life
- bit paranoid - so many different tools and no real sense of security
- Like it's a burden.
- knowledge is power. more informed
- Overwhelmed, nervous, fatigued
- Usually intimidated: I usually put off looking into it because I'm scared that I will discover I've been pwned or something really bad, but now with the guide i am more equipped to look at it deeper as putting it off only makes it worse

At this point in the workshop, we had already asked participants to think critically about their digital footprint through threat modelling. If everything went according to plan, they would then take deliberate action to improve their existing practices during the

tech support session. Responses we collected for this first discussion question therefore reflected not only different visions of cybersecurity, but also how the workshop so far had affected them. In this regard, we received a large number of positive responses. Participants said they felt "safer!", "better after today!" and "more secure, less anxious". This appears to be closely correlated with the access to information and learning that the workshop provided. One participant stated "knowledge is power. more informed", another saw cybersecurity as "less complicated once it's demystified".

While positive responses provided welcome validation of the workshops, participants also felt overwhelmed, confused, anxious, and vulnerable. Taken together, negative feelings outnumbered the self-contained positive theme, suggesting there is still much to be done in care-oriented cybersecurity. Responses such as "exhausted", "daunted", "a lot of info in one go", and "it's never ending!" point to the limitations of a three hour workshop in its ability to have a positive impact on participants while remaining digestible and realistic (more on this in the limitations section below). We observed that uncertainty and self-doubt persisted, with one participant pointing out that it's "hard to know how much is enough, it feels quite intangible", and similarly: "also not sure if im downloading things unnecessarily / can't guage the risk [sic]". While participants felt more in control after the tech support session, it appears that to feel fully empowered this must be paired with a better understanding of threats and risks.

Participants often struggled to relate to cybersecurity as an abstract concept. The pervasive feeling of being overwhelmed speaks to this, and echoes the idea of "unknown unknowns" as an obstacle to empowerment and action. Some expressed this through anxiety or a lack of trust ("the word cybersecurity doesn't feel like it's protecting you, it feels like it's against you"), others through alienation or emotional distance ("I think it's really something that I don't necessarily feel intuitively a sense of responsibility for"). Perhaps shedding light on this disconnect, a few responses lamented the lack of relatable focus in mainstream cybersecurity discourse. At the level of the individual, one participant argued, cybersecurity "is not about the worst-case scenario, it's about the everyday scenario".

A recurring theme that mostly surfaced during interviews and focus groups was that of loneliness or isolation. One participant said "I am concerned about that, but sometimes I feel alone", another brought up "an element of societal kind of shame" that places cybersecurity responsibility on the individual "if you've put stuff on the internet that shouldn't be out there". As a third participant pointed out, "we're so used to thinking about the internet as such a kind of solipsistic experience".

<u>How do personal experiences (such as gender, race, class, educational background, anything else) shape your engagement with cybersecurity?</u>

- Being a woman/nb person on the internet isn't as safe- there is panic around your device being hacked and female celebrities nudes being shared-- but because it feels like an intimidating male space, its difficult to protect yourself
- Class - private school had access to quite good IT resources and lessons
- having card cloned made me feel more paranoid

- knowing that I won't be able to afford a lawyer if something bad was to happen has limited my type of engagement with others due to feeling less safe
- Generation - I feel a lot more knowledgeable compared to my parents/ grandparents, so I don't feel as panicked ordering things online or doing online banking as they do
- I feel like women are viewed to not know anything about cybersecurity which leads to mansplaining A LOT :(
- I am more circumspect when putting opinions about race on social media than gender class or other. The threat is reputational more than anything else.
- being a part of an activist collective; feeling responsible for other's privacy

Gender was most frequently mentioned as a source of personal experience which shaped participants' engagement with cybersecurity. Many participants shared experiences of being condescended to, patronised or subjected to "mansplaining" due to their gender. Participants noted that people providing IT lessons or tech support are often male: one participant explained that "being a female getting tech support from a male can be disconcerting. Fears over what private info they might see, find, engage with … make women feel vulnerable." Feeling vulnerable was often mentioned in relation to gender, particularly with subjects like location-tracking, sending nudes and misogynistic trolling (particularly on Twitter). However, one participant emphasized that these types of threats are not necessarily about gender, as they "can happen to any person", and perpetrators of stalking or other abuse are "not only men but can be women." Participants who were women or assigned female at birth (AFAB) often described navigating the assumption that they would not be interested in cybersecurity; some wondered whether their own past lack of interest in technology was due to "social construction".

The second most common identity category was professional. Participants often learned about cybersecurity primarily in a work setting, and therefore felt they had less knowledge of their personal cybersecurity than they did of company cybersecurity policies. The need to maintain a professional reputation drove many participants' concerns for privacy and maintaining boundaries between professional and personal life, particularly for those who felt they had "more to lose" in their careers. Conversely, one participant who had been a sex worker noted that the security of her professional life was extremely important, but that she was often met with attitudes of "well you can't expect privacy when you've done that sort of work" from others. Working life can also lead to vulnerabilities. Employers having access to private communications made participants feel threatened, and participants who worked as freelancers noted they are more exposed to threats like public WiFi and receive less IT support. Experiences of employers surveilling social media —for example, through requiring Instagram handles in a job application— led many participants to implement stricter privacy controls or censor their speech online. Participants who worked with particularly sensitive data, such as anti-deportation work or online therapy, said this made them more aware of cybersecurity.

Age —the third most frequently mentioned identity category— was seen as "a huge factor" in shaping engagement with cybersecurity. Many participants described helping their parents and grandparents set up technology and worrying these older family

members might fall for online scams. Others were concerned that with an increasing number of products and services only accessible online, these services might become inaccessible to older citizens. Similarly, participants with children mentioned that concern for their children's privacy or wish to "be a good role model on this matter" had led them to seek out more information on the subject. Many participants discussed generational differences in attitudes to online privacy. One participant described being in the first generation to grow up online as a "weird double edged blade, because on one hand I'm used to monitoring how I present myself on there, but also I was on there so young that some cautionary practices were never instilled in me [...] someone who comes to being online [...] at [a] later point in their life have more critical thinking about how they're on there." This description of older people being more critical contrasted with many depictions of parents and grandparents as being naive or overwhelmed.

Experiences of privilege (or lack thereof) linked to wealth, class and education were also factors in shaping engagement with cybersecurity. Several participants framed cybersecurity knowledge as a privilege that comes with good education, as private schools have more access to IT and lessons. Being able to pay for technical or legal support if necessary is a big factor in limiting and enabling engagement online, and some tools like VPNs are expensive. Several participants hypothesized that their own privileged backgrounds had made them feel more complacent about security and privacy online. This was an unexpected finding as we had not previously considered how experiences of privilege intersect with cybersecurity.

In contrast, several participants linked experiences of being in minoritised groups —due to race/ethnicity, sexuality or gender identity— with a greater need for digital security. Participants who had been in organisations focusing on race, or just spoken out about race online, reported increased online aggression and worries about doxxing. Experiences of being queer or polyamorous online made people more aware of granular privacy settings which were necessary for "managing what I present to different audiences that have different levels of awareness of my sexuality." One participant outlined the ways in which online banking put them at risk as a trans person: they live in a country in which changing your name to match your gender identity is not legal, and their legal name is still visible through online banking, exposing them to the risk of being outed with every financial transaction they make. In this way, individual acts of harassment and seemingly neutral design choices reinforce structural forms of oppression.

Lastly, as a result of our collaboration with several activist groups, participants' identity as activists was a common consideration in shaping engagement with cybersecurity. Many participants described experiences of police surveillance at protests which made them more aware of digital privacy. Similarly, being part of activist collectives made people more likely to be concerned about group privacy as the choices of fellow activists can increase their exposure online and vice versa.

Are there any cybersecurity tools that you haven't encountered yet but that you wish existed?

When asked to invent new cybersecurity tools, participants responded with creative, sometimes hilarious and often thought-provoking ideas. We believe their contributions, detailed below, display the potential of citizen science in this area. The following list of tools is non-exhaustive and categorised according to our own interpretations.

Erasure tools:

- "Delete me" button: a button which would erase all the data the website has collected about you (this tool was suggested five separate times across the workshops!)
- "a way to quickly and easily remove sensitive information from certain parts of your devices but not necessarily erase everything"
- "something that can permanently delete old Facebook messages"

Educational tools:

- "prompts like on Duolingo to make small improvements to your cybersecurity monthly/weekly"
- "repository of" knowledge for cybersecurity where you can choose your level of difficulty

Additional controls:

- "something that covers the microphone when you close the phone- like a webcam cover"
- "text-only browser that strips all the potentially malicious add-ons"
- "privacy operating system that changes the default settings for microphone access etc"
- "ad blocks for mobiles"
- "breathaliser so that you can't send certain messages/tweets or access certain people."

Knowledge tools:

- "notification that tells you whether an ad you're viewing is targeted or not
- "a ranking website to judge how secure a website is - like the food hygiene rating!"
- "Something that summarises all data sent out and all data collected - but in an accessible summarised clear way - which could lead you to be able to send requests to stop collecting data etc"

Anonymity tools:

- "Something like WhatsApp or Signal that doesn't show your number - Telegram does this but asks your number/profile when you sign in anyway"
- "Something that generates fake data that makes me appear like I'm someone else"
- "Something which would literally create an entire second fake person, [...] just like an entire different data footprint which looks like a real person."

Streamlining tools:

- "A package that installs baseline security options"
- "Maybe something like a tool that reads [Terms and Conditions] for you and says, 'Okay, these are your concerns.'"

While this question consistently led to animated discussion, with many participants pushing back on the question: "It's more about creating norms around security than building more tools" or "better laws: tech worlds encourage tech solutions but I don't want more complex tech/buy more tools". The default should be more private than it

is, and companies should implement solutions into their products rather than expecting consumers to purchase additional technology. As one participant put it: "but these potential tools hinge around the fact that what you really want is [...] trust. Like if someone could just invent, I don't know, some way of definitely holding Facebook [or] Instagram accountable."

Should "good cybersecurity citizens" keep up to date with cybersecurity practices (such as those in the DIY Handbook)? Is this an unfair burden? If so, what are the alternatives?

- It's a big time burden that negatively impacts people who are already busy, tired, stressed or primary caregivers
- Good cyber security should be built into apps and platforms from the start as a default. But of course it's not because the business model relies on us being slack
- Those that have the privilege of knowlege have the responsibility of teaching
- I think its a mistake to leave the responsibility to institutions and laws. Whilst it is also their responsibility, I do think communities are responsible for looking after each other.
- It's not an unfair burden - but people should be more aware of why it is significant so they feel more motivated to address the issues. Education is crucial.

With this final question, we invited participants to reflect on the assumptions behind the DIY Guide and on the value of holding a digital privacy workshop in the first place. We were concerned that in doing so, we risked recreating a pattern in which solutions for cybersecurity problems rest on individuals. Many participants felt that the burden of online security should instead be placed on companies and governments Participants pointed out that we cannot expect digital privacy skills and knowledge of people that do not have easy access to them. Across focus groups and interviews, we heard concerns that wealth and education represent significant barriers: "there's obvious stuff in the sense that like VPNs cost money", and more fatalistically "perhaps 'good' cyber security is only for the privileged". There also seemed to be broad consensus that emphasising citizen responsibility often leads to victim blaming and companies "getting away" with unsafe tools and data practices. Participants felt that "big companies rely on placing the responsibility on the individual, knowing that they can abuse that when people inevitably don't take the initiative". Other responses felt they had no choice but to expose themselves to digital threats. As one interviewee stated, "everything feels so far embedded that it becomes difficult to know where to start". Similarly, a participant imagined being robbed while walking down the street: "nobody says, 'Oh, you shouldn't be going down the street'".

This suggests that solutions may not lie in better practices for individuals but by improving the safety of our digital "streets''. There was much discussion and debate around avenues for achieving this, touching on legislation, companies and culture. There were many suggestions of "accreditation" systems, "reviews", and "restrictions". The topic of GDPR surfaced in several conversations, as a good starting point for ensuring companies are given "the right incentives". Others suggested better information and guidelines at the user level: "Stricter laws around minors using the internet - kids are stupid and thats ok, the law should protect them and their data," one participant wrote. Legal reform and increased platform responsibilities were particularly important for survivors of intimate image abuse: participants felt the law should

recognise this as a form of sexual abuse, afford survivors the same protections as survivors of offline sexual abuse, and prosecute platforms which continue to share the abusive images. Platforms should offer filters and controls to limit harassment, which would help create safe online spaces for survivors and, by extension, everyone else.

Building on the idea of shared responsibility between state, companies and people, another participant referred to the metaphor of healthcare: "The moment you start realising what the risks are for specific things, then you start taking steps. As long as the state or even the private sector, if they make available for you, the tools to protect your health, then you will do it." This was echoed by many responses expounding the desire to build a more caring society with the premise that "data protection is a human right!!" Participants argued that "cybersecurity should be in the schools curriculum", and "some sort of like separate bubble of judgement free education is quite important".

Although policy and regulations appeared to be intuitively important to participants, many struggled to see companies or states as sources of help and positive change. "There's always so much chat from websites like Facebook about all this", one interviewee complained. "I got one from Google the other day about 'we've updated your privacy settings'. It's all just, it seems like a lot of lip service." Another commented that "I think its a mistake to leave the responsibility to institutions and laws. Whilst it is also their responsibility, I do think communities are responsible for looking after each other."

Responses like these introduced the interesting theme of group privacy. Participants often and completely unprompted returned to the notion that their security is connected to the security of others: "I guess I am linked to other people digitally". Many felt that "we can make it a more collective thing because it has so many collective benefits." Indeed, we saw this first hand in the workshop feedback, as participants reported improvements in their levels of confidence after discussing and sharing their experiences with others. There were also many comments on how improving security for yourself improves security for others: "I would just love everyone to be super secure because it helps other people to be secure as well". Through this lens, we see promising horizons for community-based projects like Reconfigure.

Special Workshops

We conducted four workshops in partnership with activist and community organisations, namely: Oxford Extinction Rebellion[32] (XR), Power Play[33] (a feminist activist theatre group) in collaboration with Victims of Image Crime[34] (a group of survivors of image-based sexual abuse), the Edinburgh Anarchist/Feminist Book Fair[35], Common Ground[36] (a coffee shop and social enterprise that serves as a hub for community events) and People & Planet[37] (a student environmental campaigning organisation). The first three of these workshops had some additional questions tailored to the groups' activities and values, which allowed for targeted discussions addressing their specific needs.

[32] https://www.xroxford.org/
[33] https://www.powerplaytheatre.com/
[34] https://voic.org.uk/
[35] https://edinburghafb.org/
[36] https://www.commongroundstudy.space/
[37] https://peopleandplanet.org/

The Oxford XR workshop discussion focused primarily on security during protests, in particular mobile phone messaging services. Participants emphasized the need to protect more vulnerable members of their groups, and collated a list of recommendations for their wider community, including training on how to use secure messaging apps, not disclosing information like phone passcodes to the police during arrests, and setting up and using burner phones. In the Power Play/Victims of Image Crime workshop, participants discussed their shared experience of abuse, as well as their preferred legal, cultural, educational and technical routes to addressing the problem. Their recommendations for legal reform were submitted as part of the UK Law Commission Review on Image-based Sexual Abuse. They emphasized the importance of controls (such as filters and blocking abusive users) and the responsibility of both technology companies and legislators to protect and promote consent in intimate data sharing. Lastly, in the workshop with the Edinburgh Anarchist/Feminist Book Fair, participants explored the questions "Can cybersecurity be anarchist? Can it be feminist?" and highlighted the need for de-centralised and community-driven security following the tenets of mutual aid.

Reflections & Limitations

Participatory action research is an iterative process that is predicated on "learning by doing."[38] It is also, as the same authors so aptly wrote, "often a messy business". We upheld the core principles of our methodology by gathering feedback during the workshops and conducting follow up interviews. In this section, we reflect on this project by reviewing participant commentary as well as our thoughts on limitations.

Participants' feedback on the workshops was mostly positive: in particular, participants enjoyed the informal, social and interactive nature of the workshop. It should be noted that there may be a selection bias at play, as those with the most positive experiences of the workshops were more likely to opt in to follow up interviews. Many participants mentioned enjoying the Mentimeter features which allowed them to respond to questions and see others' responses. Hearing other people discuss their own personal lives made cybersecurity "a lot more accessible and […] less of a chore." Participants also mentioned enjoying the action research part of the workshop, saying that "knowing that what you guys are trying to do is also to benefit other people, even though you want to gather the data, it made me feel part of a useful thing, a useful project."

Participants identified three main barriers to inclusion in addressing cybersecurity issues: a lack of motivation or "avoidance", a lack of understanding or "awareness", and exclusionary language. Many participants described cybersecurity as intimidating or overwhelming. As one participant put it: "I think there is a part of me that doesn't want to check where all my passwords are stored for fear of finding out that they're—I don't know—in the wrong place or something." Another said, "Like I don't want to deal with it, it'll be an admin task and if it goes well, nothing will happen so there's no immediately obvious reward." The fear of what you might discover by learning more

[38] Kemmis, McTaggart, and Nixon.

about your own online security —and the perceived low rewards to taking action—act as a strong barrier to engaging with this issue.

Similarly, many interviewees identified a lack of knowledge and awareness as barriers to public participation. One participant described this problem powerfully: "I think even understanding that data belongs to you and that data is valuable […] can be hard when it [...] feels like breathing. And the fact that your breathing is monetised on the internet [...] for the want of a better word is weird to get your head around." Other participants described struggling to understand, for example, the links between password reuse and data breaches, or how online monitoring works. Many participants in both workshops and interviews called for increased IT and cybersecurity education to remedy this.

Lastly, exclusionary language came up again and again as a significant barrier to participation. One participant said "Often tech help websites seem like they are written by men who are tech experts and not easy to understand." Often this exclusionary effect was attributed to "cybersecurity" or the prefix "cyber" itself: "the word cyber has been so kind of male prevalent and male dominant that [...] Like even for myself as a man, like the word cyber immediately kind of puts you off or makes you feel like it's not really a space that you have to know very much about". Furthermore, one participant noted that those resources which do exist are often not only full of technical language, but also in English and therefore not accessible for speakers of other languages.

A finding we are particularly pleased to report is that participants specifically stated that our workshops helped mitigate all three of these barriers. Addressing security in a social, supportive space allowed people to discuss and confront problems which were "kind of left unsaid" or a "bit of an elephant in the room". Participants reported that with accessible resources like the DIY Guide to hand, they felt better equipped to deal with these issues. As one participant described it, the "atmosphere we had in the workshop" helped create "confidence in hearing various tech terms and not being scared by them as such."

Wherever possible over the course of the project, we attempted to adjust for emerging flaws and incorporate everything we learned along the way. While we can happily say that our approach was a success in many of its ambitions, we also see what could be improved, and the limitations inherent to the project.

At the point of data collection, we found that participants would sometimes come to workshops looking for straightforward advice and answers. As "cybersecurity experts", it was sometimes challenging to walk the line between empowering and lecturing. During workshops, our preferred approach was to share our experiences and recommendations without telling people what to do. However, a few participants wished they could have been instructed more clearly, indicating a tension between avoiding a top down experience and ensuring that participants leave the workshop feeling that they have learned something. Going forward, this is a balance we will continue to strive for.

When asked what they would have wanted to learn more about, several participants mentioned the socio-economic aspects of data collection, such as how it creates profits for businesses. This would be an interesting subject to include in future workshops; focusing primarily on individual practices and improvements may have obscured

structural aspects of online tracking and privacy. Several also expressed interest in finding out more about the theory and reasoning behind the workshops, particularly its connection to feminist theory.

As mentioned in the methods section, some of our research design choices resulted in a less participatory methodology. The core of PAR is for knowledge to be built collaboratively between researchers and participants, but this was not always possible. At the workshops, we asked if participants would be interested in contributing to data analysis, and circulated an initial draft of this report as an open invitation for feedback. We also hired three research assistants with whom we attempted to maintain a non-hierarchical relationship. Unfortunately, no participants came forward to help with data analysis, or provide comment on the report. Furthermore, due to COVID-19 we extended the project by six months, and our research assistants moved on to other ventures before this phase was complete. To some extent, this flaw was inherent to research design rather than execution: true participatory research is co-designed in collaboration with participants, whereas we wrote the research design at the grant application stage with a smaller group of just three researchers. In the future, we plan to co-create workshop plans with project partners from the start.

Beyond research design, we also faced limitations related to recruitment. Because of our own environments (privileged academic circles), the nature of our partner organisations (often catering to millennial, tech-savvy audiences) and the locations of the workshops (urban spaces connected to academic institutions), we found an overrepresentation of participants from relatively privileged educational backgrounds who were already comfortable with technology.

Finally, a limitation that emerged from discussions with participants (informally during the workshops but equally during follow up interviews), was the standalone quality of the workshops. Many participants were happy to have a space allocated to improving their digital practices, but admitted that they didn't always make significant changes beyond it. This leads us to believe that the value of our workshops would be greatly increased by holding recurring events. Ultimately, the challenges we faced provide valuable points of focus for shaping further forays in this area of research and activism.

Conclusion

This report summarises the first stage of the Reconfigure project, in which we piloted a form of action research in which digital privacy workshops are paired with data collection in order to better understand the online threats individual citizens face, barriers which prevent them from accessing or acting on cybersecurity guidance, and solutions they would like to see implemented. At this stage, we would like to leave the reader with four impressions:

First, the enthusiasm and thoughtfulness of our participants stands in stark contrast to the stereotype of lazy, uninterested technology users, which is all too common in cybersecurity narratives. Our participants cared not only about their own digital privacy, but also about the security of their families and communities. They were curious and critical of the broader structural forces which shape online data collection and offered a wealth of creative ideas towards improving technology through product design as well as regulatory and social changes. Most people see the digital devices that shape their lives as predefined tools: to be purchased, learned, put to use, tolerated, loved or

avoided. Only a select few —technologists and designers— see them as malleable code that can be constantly improved and reimagined. These findings suggest that if more people can see themselves as agents of computing and adopt this mindset of reconfiguring, we could propose a different, more inclusive vision of what computing and cybersecurity could be.

Second, we wish to emphasize the benefits of our methods. Creating a social, supportive space for people to reflect on cybersecurity and take action helped participants identify and, to some extent, overcome common barriers. Our interactive platform helped make data collection a collaborative process where participants commented on each other's contributions, noting similarities and differences to their own experiences and putting them in the position of citizen scientists.

Third, in answer to our central research question, the cybersecurity that emerges from this project is a communal practice —one in which individuals and communities take the time to protect themselves and each other through reflection and action. These actions can be small and personal —like downloading a password manager— however it is clear from our discussions that the burden cannot be borne by individual citizens alone. Significant changes need to come from government and corporate actors taking more responsibility over citizens' privacy and autonomy.

Fourth, this *reconfigured* cybersecurity is more sensitive to the intersecting experiences of privilege and discrimination that inevitably shape life online. By taking these diverse standpoints and perspectives into account, we learn about a wider number of threats which affect people who have a different set of experiences to the average cybersecurity expert. By respecting these experiences as a valid source of knowledge about cybersecurity, we challenge a monolithic, orthodox understanding of what "counts" as a cybersecurity issue.

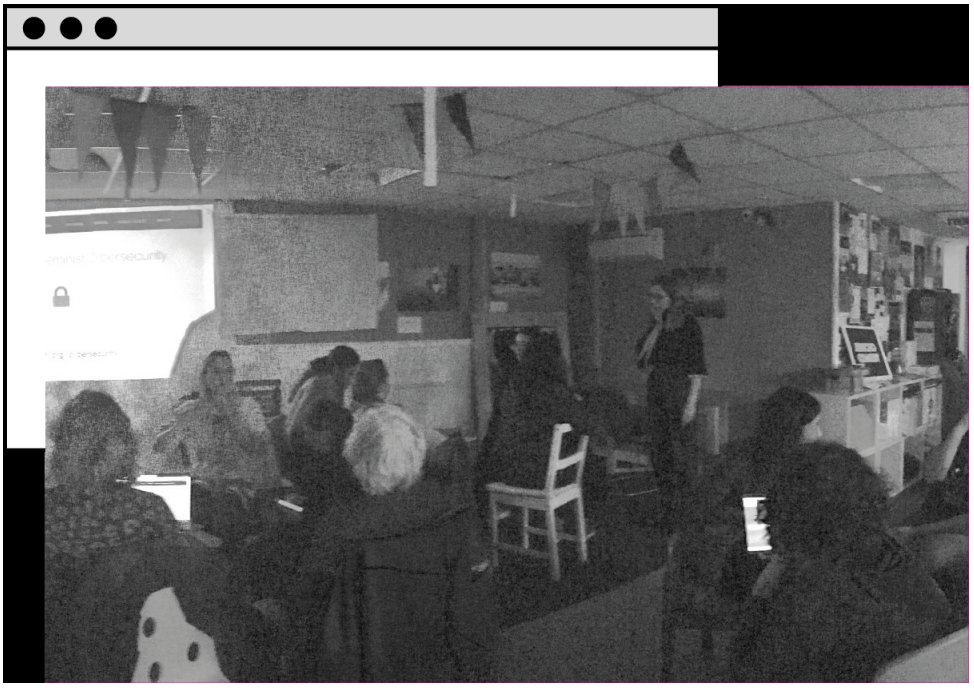
Going forward, we will publish a more in-depth exploration of our data in an academic paper. We also wish to improve on these methods by setting up a project with recurring workshops, to give participants more space and time to implement the changes they want to see. Lastly, we aim to reach out to communities which are disproportionately targeted by online surveillance and harassment. We will make these future workshops less focused on individual actions and tool-based solutions, and more aimed at developing community and finding structural solutions.

We hope this project seeds change on multiple levels. In the short term, we believe our workshops empowered participants to improve their own cybersecurity practices and engage critically with the concept of cybersecurity. More broadly, our research demonstrates an alternative approach to researching and implementing cybersecurity. We hope to see a popularisation of these methods and those of like-minded researchers as a path to democratise cybersecurity.

Please follow us on social media or join our mailing list if you would like to be updated with future projects!

Twitter: @reconfigure2020

Mailing list: https://lists.riseup.net/www/info/reconfigure



Works Cited

(ISC)², *(ISC)² Cybersecurity Workforce Study: Women in Cybersecurity*, 2019

Adams, Anne, and Martina Angela Sasse, 'Users Are Not The Enemy', *Communications of the ACM*, 1999 <https://doi.org/10.1145/322796.322806>

Braun, Virginia, Victoria Clarke, Nikki Hayfield, and Gareth Terry, 'Thematic Analysis', in *Handbook of Research Methods in Health Social Sciences*, 2019 <https://doi.org/10.1007/978-981-10-5251-4_103>

Coles-Kemp, Lizzie, Debi Ashenden, and Kieron O'Hara, 'Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen', *Politics and Governance*, 2018 <https://doi.org/10.17645/pag.v6i2.1333>

Coles-Kemp, Lizzie, Rikke Bjerg Jensen, and Claude P. R. Heath, 'Too Much Information: Questioning Security in a Post-Digital Society', 2020 <https://doi.org/10.1145/3313831.3376214>

Collins, Patricia Hill, *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment* (Routledge, 1990) <https://doi.org/10.2307/2074808>

Costanza-Chock, Sasha, 'Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice', in *DRS2018: Catalyst*, 2018 <https://doi.org/10.21606/drs.2018.679>

'During the Pandemic a Digital Crimewave Has Flooded the Internet', *The Economist*, 2020 <https://www.economist.com/international/2020/08/17/during-the-pandemic-a-digital-crimewave-has-flooded-the-internet>

Eitzel, M V, Jessica L Cappadonna, Chris Santos-Lang, Ruth Ellen Duerr, Arika Virapongse, Sarah Elizabeth West, and others, 'Citizen Science Terminology Matters: Exploring Key Terms', *Citizen Science: Theory and Practice*, 2017 <https://doi.org/10.5334/cstp.96>

Haraway, Donna, 'Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective', *Feminist Studies*, 1988 <https://doi.org/10.2307/3178066>

Harding, Sandra, 'Feminist Standpoint Epistemology', *The Gender and Science Reader*, 2001

Hesse-Biber, Sharlene, Patricia Leavy, and Abigail Brooks, 'Feminist Standpoint Epistemology: Building Knowledge and Empowerment Through Women's Lived Experience', in *Feminist Research Practice*, 2012 <https://doi.org/10.4135/9781412984270.n3>

Kemmis, Stephen, Robin McTaggart, and Rhonda Nixon, *The Action Research Planner: Doing Critical Participatory Action Research*, *The Action Research Planner: Doing Critical Participatory Action Research*, 2014 <https://doi.org/10.1007/978-981-4560-67-2>

Kindon, Sarah, Rachel Pain, and Mike Kesby, 'Participatory Action Research: Origins, Approaches and Methods', in *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*, 2007

McMahon, Ciarán, 'In Defence of the Human Factor', *Frontiers in Psychology*, 11.1390 (2020)

Mehta, Ivan, 'A Look at How Jitsi Became a "Secure" Open-Source Alternative to Zoom', *The Next Web*, 2020

<https://thenextweb.com/apps/2020/05/21/a-look-at-how-jitsi-became-a-secure-open-source-alternative-to-zoom/>

NCSC, *Decrypting Diversity: Diversity and Inclusion in Cyber Security*, 2020

Redmiles, Elissa M, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, and others, 'A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web of California San Diego', *USENIX Security Symposium*, 2020

Riach, Kathleen, 'Exploring Participant-Centred Reflexivity in the Research Interview', *Sociology*, 2009, 356–70 <https://doi.org/10.1177/0038038508101170>

Slupska, Julia, 'Safe at Home: Towards a Feminist Critique of Cybersecurity', *St Antony's International Review*, 2019

UK, Glitch, *The Ripple Effect: Covid-19 and the Epidemic of Online Abuse*, 2020 <https://fixtheglitch.org/covid19/>

Appendix 1: Data Analysis Codebook

Data structure

Types of data:

1. Mentimeter form
    a) Demographic/multiple choice questions: gender, age, skills
    b) Free form responses
1. Focus group transcript
2. Interview transcript

Coding protocol

Two coders will code each data type (i.e. mentimeter form, focus group transcript, interview). Each coder will follow the followings steps:

1. Familiarise yourself with the codebook
2. Read over the data once
3. Note down initial thoughts
4. Read over the data again, categorising each entry according to "topic" and/or "theme". Not every data entry needs to have both. Every data entry can have multiple topics and themes.
5. Hide your codes using the Excel "Hide" function so as not to bias the second coder
6. With the other coder, standardise your responses and enter them into "Aggregate Data"
7. Any remaining disagreements should be moderated by a third coder
8. Add to the codebook if all three coders agree change is necessary

Topic Codes

Initial codes

Code name	Explanation	Example
Targeted advertising	Desire to avoid targeting, description of experience of being targeted	"How to stop being targeted by crappy Amazon ads" "Convincing spam" "biometric targeted ads"
Password	Desire to improve password security, get a password manager. Descriptions of difficulties of keeping track of passwords	"To learn what a password manager is and how they work" "Having to go through all the sites you have used with the same passwords is a pain."
Account spread	Descriptions of account hacking, difficulties of keeping track of accounts, tools that enable keeping track of accounts	"a tool that unsubscribes you from all the websites so you dont have to go individually"

Encryption	Explicit mention to encrypting data such as messages or hard drive	
Photos	Protecting images or video	
Financial	Protecting financial data, bank account details, descriptions of financial breaches	"I'd rather have my bank accounts emptied than all my private messages aired and shared"
Private messaging	Protecting messages in email, social media, or instant messaging platforms	"I'd rather have my bank accounts emptied than all my private messages aired and shared"
Reputation	Protecting reputation (i.e. in social media)	
Location tracking	Protecting location, identifiable information	"My phone sharing my location without me opting in"
Algorithmic inferences	Protecting against inferences made related to data trails, protected identity characteristics, online tracking, digital footprints	"Information related to protected characteristics that appears to be 'scraped' from multiple sources"
Biometrics/ Facial recognition		"biometric targeted ads" "Face-recognition on facebook"
Video surveillance	Being recorded in public or private spaces	"Doorbells acting as CCTV by proxy"
Unsolicited messages	Experiences of unsolicited messages or harassment (more of a one off from a person or group of people); phishing emails	"Messages from weirdos"
Stalking	Worries or descriptions of stalking (persistent contact/surveillance from one person)	"Being stalked by strangers or friends of friends and finding boundaries between being polite and being safe" "Directly threats on twitter messaging from weirdo stalkers"
Anonymity	Anonymous browsing	
Contracts	Social media terms & conditions	"Knowing what T&C's I agree to"

Screenshot	Descriptions of using or defending against the screenshot tool	"a snapchat but more efficient so if you send a photo it will be deleted & can't be snapshotted"
Misc/outlier	Something which does not fit in other categories/is difficult to understand what they meant	

Emergent codes

Mobile phone	Mobile phone security: protecting phone numbers, mobile pin codes, mobile app specific concerns	"Mobile phone on demonstrations."
Online tracking	Combines targeted advertising and algorithmic inferences Desire to avoid targeting, description of experience of being targeted	"How to stop being targeted by crappy Amazon ads" "Convincing spam" "biometric targeted ads"
Harassment	Descriptions of unwanted, abusive or distressing online communication, especially if repeated or targeting protected characteristics, including hate speech	"Zoom meeting was hacked by immature boys in masks showing silly things they thought were disturbing."
Malware	Viruses & malware	"Trolling, scams, malware."
Deletion	Descriptions of deleting data, or difficulties, struggle or desire to delete data	"I have a question on this. If someone had inputted that, even if you delete some photo, x, y, z thing required. There is always a footprint that is left behind on the web. So, there is no assurity your complete data is gone"

Theme Codes

Initial codes

Code name	Explanation	Examples
Intimacy	Desire to protect intimate data, threats created by intimacy/intimate relations like family or dating	"The presence of my Chinese aunties online is pretty terrifying"

Autonomy	Desire for greater autonomy	"getting out of random websites i signed up for in the past"
Controls	Desire to control who sees what information at what time, get greater control over using devices	"Only things I opt 'in' to share should be publicly available" "I think a lot about what is visible to different audiences"
Knowledge	Desire for more knowledge, difficulties due to lack of knowledge	"something that automatically googles a number that calls you so you know who it is"
Feeling:Overwhelmed	Feeling overwhelmed, hopeless, daunted or powerless: impossible time burden. Feeling uneducated or inadequate.	"so many different tools and no real sense of security" "It's neverending!"
Feeling:Anxious	Explicit mention of feeling anxious, stressed	
Feeling:Frustrated	Feeling frustrated, exasperated, description of unnecessary burden	"Initially - stupid. Then - frustrated. Later - smug... or a failure depending on the outcome. After - paranoid."
Feeling:Confusion	Feeling confusion and/or uncertainty about what is important, what you need to know, whether any of this is necessary,	"i don't really know what i don't know" "is it overkill? does anyone want my tweets and emails?"
Feeling:Avoidance	Not wanting to deal with it, procrastination	"Like I don't want to deal with it, it'll be an admin task and if it goes well, nothing will happen so there's no immediately obvious reward."
Feeling:Paranoia	Feeling watched/listened to, not knowing which threats are real, mentioning *not* wanting to feel paranoid	"Incursions into private messaging - perception of being listened in on by FB across multiple platforms"
Feeling:Lack of trust	Lack of trust in the companies handling of their data, in the system architecture, in users Lack of trust in themselves or the government	"perception of being listened in on by FB across multiple platforms" "Information related to protected characteristics that appears to be 'scraped' from multiple sources"

Feeling:Guilt	Guilt about bad practices/laziness, negligence	"My own laziness about checking privacy setting and what I give away freely"
Feeling:Positive	Feeling positive about cybersecurity, whether due to workshop or other reasons	"Better after today!"
Feeling:Outlier	Outlier feelings such as nostalgia, feeling patronised or annoyed	"nostalgic - passwords reflect different parts of my life" "It's definitely a realm where I've been patronised."
Feeling:Vulnerable	Feeling vulnerable	"Being a female getting tech support from a male can be disconcerting. Fears over what private info they might see, find, engage with that make women feel vulnerable."
Identity:Gender	Gender-related intimidation, feeling "other"ed in tech support or unfamiliar in male-dominated spaces	"Being a female getting tech support from a male can be disconcerting."
Identity:Age	Comments related to age or generational difference	"Generation - I feel a lot more knowledgeable compared to my parents/ grandparents, so I don't feel as panicked ordering things online or doing online banking as they do"
Identity:Profession	Comments related to how professional life shapes people's identity or experience	"Working within academia, I think a lot about the boundaries between personal and professional"
Identity:Sexuality	Comments related to how sexuality shapes people's identity or experience	"Sexuality - managing what I present to different audiences that have different levels of awareness of my sexuality"
Identity:Race		
Identity:Outlier	Comments related to an identity other than race, gender, age, profession or sexuality	
Experiences of attack	Experiences of attacks changing perceptions of	"having card cloned made me feel more paranoid"

	cybersecurity, also experiences of tracking/privacy violations	
Solutions:tools	Solutions involving new technology tools, devices, platforms	"a face blurring tool so that it is recognisable to a human eye but not an algorithm"
Solutions:legislation	Solutions involving the state or laws	"better laws: tech worlds encourage tech solutions but i don't want more complex tech/buy more tools"
Solutions:culture	Solutions involving education or culture change	"cybersecurity should be in the schools curriculum"
Solutions:company	Solutions involving company responsibility, or obstacles to companies addressing the issue	"Good cyber security should be built into apps and platforms from the start as a default. But of course it's not because the business model relies on us being slack"

Emergent codes

Identity:activist	Comments related to how activism shapes people's identity or experience	
Identity:education	Comments related to how education shapes people's identity or experience	"Educational background is the most important factor"
Identity:class	Comments related to how class shapes people's identity or experience	"Class - private school had access to quite good IT resources and lessons"
Reflections on cybersecurity	Comments reflecting on the definition, meaning or broader function of cybersecurity in society	"the word cybersecurity doesn't feel like it's protecting you, it feels like it's against you"
Reflections on workshop	Comments reflecting on experiences of the workshop, constructive criticism	"Yeah, I really enjoyed it, it was definitely very new for me as a subject I guess or a thing to both learn about and discuss-- sometimes a bit

		conceptually, or from a particular lens, especially through a feminist lens."
Responsibility	Whose responsibility is cybersecurity?	"That makes me feel like it's not relevant to me, which I know is not true and I realise that it's certainly not true. But I think it's really something that I don't necessarily feel intuitively a sense of responsibility for."
Group privacy	Comments reflecting on communal aspects of security, taking care of others or how other's actions affect you	"being a part of an activist collective; feeling responsible for other's privacy"
Language	Language as a barrier to access	"Despite privilege in terms of the classification I find the language intimidating and difficult to address"