Stronger NYC Communities Organizational Digital Security Guide

Facilitator Guide

Build Power - not Paranoia!

This work supported by Mozilla Foundation, the NYC Mayor's Office of Immigrant Affairs, NYC Mayor's Office of the CTO, and Research Action Design.

CREDITS

Project designed and lead by **Sarah Aoun** and **Bex Hong Hurwitz.**
Curriculum lead writing by **Rory Allen**.

Workshops, activities, and worksheets were developed by **Nasma Ahmed**, **Rory Allen**, **Sarah Aoun**, **Rebecca Chowdhury**, **Hadassah Damien**, **Harlo Holmes**, **Bex Hong Hurwitz**, **David Huerta**, **Palika Makam (WITNESS)**, **Kyla Massey**, **Sonya Reynolds**, and **Xtian Rodriguez**.

This Guide was arranged and edited by **Hadassah Damien**, and designed by **Fridah Oyaro**, Summer 2018.

More at: **https://strongercommunities.info**

Table of Contents

ORGANIZATIONAL DIGITAL SECURITY GUIDE

This guide provides tools and ideas to help organizational digital security workshop leaders approach the work including a full facilitator's guide with agendas and activities; for learners find a participant guide with homework, exercises, and a resource section.

02

FACILITATOR GUIDE 37

Facilitation Agendas, Exercises & Handouts

1. Stronger NYC Communities Workshop: **Principles and basics of holistic security**
2. Stronger Communities Workshop: **Data Stewardship and Security**
3. Stronger Communities Workshop: **Organizational Security as a Team + Topical Open Spaces**
4. Stronger Communities Workshop: **Our work is about learning from and taking care of each other.**
5. Stronger Communities Workshop: **Incident Response Strategies & Series Wrap-up**

Workshop 1
FACILITATOR GUIDE

WORKSHOP 1: OUR WORK IS POLITICAL.

Principles and basics of holistic security

Learning Objectives

- Our work is political
- Build a shared understanding of how politics and power shape the technologies and practices of surveillance
- Discuss and share strategies for using collective action to shift the design of technologies and practices of surveillance
- Understand shared experiences and shared challenges/ opportunities
- Develop risk assessment as a tool to bring back to each organization
- Build knowledge about reducing unauthorized access by using strong passwords, password managers, and 2FA as tools and tactics to bring back to each organization
- Understand how to use 2-factor authentication and storing backup codes
- Understand how to use a password manager
- Recognize phishing attacks and identify ways to change phishing-vulnerable behavior (if time)

3 hours

Activity	***Time (3 hours)***
Greeting and overview	***5 minutes***
Introductions	***35 minutes***
Building Political Power: Empire, Colonialism, and the History of Surveillance	***20 minutes***
Break	***10 minutes***
Holistic Security Process: Risk Assessment	***45 minutes***
Tactics and Tools: Account Access and Management (includes a break)	***55 minutes***
Questions, support, to-do's	***15 minutes***

Materials and Prep:

Print preparation

- Print the Risk-assessment Activity at the end of this Guide section
- Print the Participant Handout

Room set up needs:	Materials to print and prepare	Activities
Name tags, markers, Post its	List of Agreements - Bring the agreements from the Design section, or create your own. Create an area on a whiteboard or piece of paper for agreements.	Introductions
Light snacks	Homework handout	*Building Political Power overview*
Whiteboards or big paper	Evaluation	Holistic Security Process: Risk Assessment
Seating, set up in a circle, extra chairs if possible	Parking Lot: Create an area on a whiteboard or piece of paper for questions and issues to follow up.	Account Access and Management: Passwords and 2FA
Projector		

1. Greeting and overview

5 min

Documentation: Assign a documentation person and share these pieces at the end of a workshop with the trainers list

Parking Lot: Create an area on a whiteboard or piece of paper for questions and issues to follow up.

The purpose of this section is to introduce trainers and participants face to face, to share about who they are and to orient the room around the project overview and roadmap.

Trainer - Introduce motivation for the project

- Introduce the project partners

Review Program Goals

- review the goals and thank participants for participating in assessment process to design this series

Review Workshop Agenda

- Review the agenda
- Introduce the curriculum themes that will recur throughout the the workshops

2. Introductions

Personal introductions

Introduce the project and the partners involved. Introduce yourselves (trainers), and invite participants to introduce themselves.

- Name, where you work; why you are here

Collective commitments

Encourage participants to suggest collective commitments. They should be honored for the duration of the project that should reflect the values and hopes of participants and trainers, and could include things like:

- **Everyone is an expert:** the implementing team, trainers, and participating organizations all have valuable skills, knowledge, and experience to share. We are committed to making space and creating activities that allow all to share their expertise. We are committed to crediting all contributors.
- **What's learned here leaves here, what's said here stays here:** when we leave this space, we share learnings, not personal details and stories;
- **Accessibility:** We welcome questions and are committed to using accessible language
- **We respect each other's time and attention:** punctuality, missing sessions, let Sarah and Bex know, communicative
- **We consider security holistically:** the practices that are developed should be sustainable, should contribute to a sense of organizational self-care, longevity and groundedness, and should honor and reinforce the organization's goals and needs.
- **This work is political:** racism and the practice of mass surveillance are interwoven with colonialism and the apparatus of the state. A goal of these workshops is to build political power and understand how movement-building and collective action are as much a security strategy as any technical tactics.

35 min

Additional materials

Large paper + markers

The purpose of this section is to begin to build some familiarity with each other and develop collective commitments about how we will share this space.

Trainers' notes

- Write the commitments down on a large piece of paper as the group comes up with them. They can be reviewed briefly at the beginning of each month's workshop (maybe you want to add some as time goes by!).
- Also, if you encounter someone who is disrupting/dominating the workshop or causing some other kind of conflict, referring back to any commitments you made together about group respect is a way to keep things on track. Save these commitments for the subsequent workshops.

3. Building Political Power: Empire, Colonialism, and the History of Surveillance

Discussion: Grounding in the work of people in the room
Ask participants

- How is your organization addressing community safety and systems of surveillance?
- How have the communities you work with been surveilled by the state?
- How have these communities resisted these surveillance practices?

Document - Write down on a large piece of white paper – photograph this at the end of the workshop and send to the list

Presentation: History of Surveillance
Overview

- The history of surveillance is closely linked with institutional racism, colonialism, and the expansion of US imperialism.
- Certain practices, such as the 18th century lantern laws, have echoes in today's surveillance apparatus. Think of Stop & Frisk, and Omnipresence.
- Most technological advances in history have been tied to their use for the control, monitoring, and surveillance of populations.
- Understanding how these tools have been used historically for controlling populations allows us to adopt a critical and intersectional lens on present-day practices (disclosing social media at border, stop & frisk, mug shots, biometrics scans, etc.)
- Risks of using social media apps: data exchanged or mined by law enforcement. Examples: predictive policing, City of NY ID cards, Muslim registry, etc.

20 min

Break: ***10 min***

Additional materials

(Optional) handout or additional resource for trainers,
"W1 - Empire, Colonialism, and the History of Surveillance."

Trainer notes

- This session can spark a lot of discussions, you may need to be mindful of the time.

Break 10mins

The purpose of this section is to ground this workshop and program in a political and social understanding of surveillance and security. We begin with discussion to make space for participants to introduce parts of their work already addressing community safety and systems of surveillance.

4. Holistic Security Process: Risk Assessment

Introduction to holistic approach

- Political, organizational, personal, technical, social, physical, emotional.
- Security doesn't exist in a vacuum; the work we are doing is people-focused, and the strategies we use to build our resilience in this work also have to meet the needs of us as both a collective and as individuals. Trying to impose exogenous security measures that don't reflect our needs and values as political beings does violence to ourselves, our organization, and our collective sense of strength.
- On the other hand, presenting a few paths and choosing for ourselves and our organizations which tools or tactics reinforce our existing strengths and speak to our needs and goals makes new practices easier to adopt, more likely to stick, and (ideally) lend them more positive emotional resonance than adopting someone else's practices out of fear.

50 min

Additional materials

For trainers, "W1 - Emotional aspect of holistic security."

Discussion: Begin Here

Implementing change in a group is not simple. No matter where you organization is in its process – if you are bringing this back for the first time or updating a 20 year old security policy, grounding this work in your organization's values and vision will be one way to ensure that your policies and best practices will be aligned with your organization's values.

We suggest these questions.

- What does 'safety' look and feel like for you?
- What are your organization's values and vision?
- What makes your organization or the movements you are a part of powerful?

Building Resilient Strategies Starts with Risk Assessment

- We manage risk every day:
- Locking office doors
- Using passwords on phones
- Cross the street using a crosswalk
- Updating our softwares
- Brushing our teeth

The purpose of this section is to introduce the holistic security process we will follow from Workshop 1 through 5 to develop organizational policies and best practices. We introduce questions to ground holistic security processes in organizational values and vision and then introduce Risk Assessment because as the first process.

Background: The motivation for risk assessment

As much as risk assessment is to discover 'what assets you have and who you want to protect them from,' the most important feature about risk assessments is that they are specific and constrained. Vague, amorphous worst-case scenarios lead to stress, defeatism, and inaction. On the other hand, good, specific risk assessments hone in on particular areas where decisions around security can be made and and organizations' power around their security decisions can increase.

Risk assessments provide a tool for participants to bring back to their organizations to bring about this specific, directed thinking. This is the first step in developing policies and best practices.

Discussion

Discuss and explain risk assessment with examples. Begin by providing a short walkthrough of a simple risk assessment, then suggest another example and open up to participants to fill in (some off) the scenarios.

Group Discussion: Risk assessment in our own organizations

- If there is time, it may make sense to work in pairs or groups of 3, and come up with 1 or 2 very specific assessments per group.

- If there is not time, explain that participants can facilitate the Risk Assessment as a large group or ask people to work in small groups or papir and shareback.

Trainer notes

Try to encourage a variety of topics so that the assessments can be shared back to the group.

Additional Materials

- (Optional) Handout "H4: Risk Assessment Walkthrough" for an example scenario and subsequent prompts if folks don't want to discuss their own circumstances (but hopefully they will!).
- Risk Assessment questions will be noted in participant handout.

5. Tactics and Tools: Account Access and Management

55 min

Includes
Break: ***10 mins***

The purpose of this section is to introduce tactics and tools for managing account access and phishing.

We cover:

- **Strong Passwords**
- **Password Managers**
- **2-Factor Authentication**
- **Phishing Training**

Motivation: Why is this important?

Our first lines of defense against: data/information leaks, impersonation, fraud, disruptions to our workflow… you name it.

Hands-on: Strong passwords

In this section we will review some of the tools participants may already be using, such as a password manager, and will walk through setting up 2-factor authentication and saving backup codes.

Activity: Choosing a password manager

Activity: Setting up 2-factor authentication
setting up / requiring 2FA and password managers
downloading and safely storing backup codes

(If time) Discussion: Phishing

Now that we have long, secure passphrases, 2FA, and a password manager to tie it all together, we don't want to get phished. In this section we will review what phishing is, see some common phishing attacks, understand the difference between targeted and non-targeted phishing attempts, and learn how to reduce the risk of getting phished.

Discussion: Phishing & Malware

- What makes a suspicious email? Invite participants to make a list of signs to watch out for.

- Why do we care about phishing? Among other things, the risk of downloading malware. What can malware do? How can we deal with it?

Trainer notes

See "A note on organizational culture and phishing" (W1 H3), emphasizing that the best way to protect against phishing is for your natural habits to be as 'un-phishy' as possible so that phishing attempts stick out as strange/atypical when they do arrive.

6. Questions, support, to-do's

Review & homework for next time

We have discussed some strategies to:
- choose a secure password
- set up 2FA and back up your codes
- conduct risk assessments
- create organizational commitments

(And maybe we also talked about ways to:)

- minimize the risk of getting phished
- foster a digital communication culture that makes phishing behavior stand out

Homework: There are 3 activities (see handout)

- Risk assessment exercise
- Password manager/2fa exercise
- Rating tools and tactics: which ones sound like tools you can adopt? Which ones sound like there will be barriers to adoption? Why?

Additional Materials

For participants: refer to handout from their Workshop 1 Participant Guide "Homework: Checklist + Risk assessment".

15 min

Trainer Notes

Use the remainder of the time to be available for 1-1 support, specific questions, and suggestions. Since each trainer may receive different feedback, all trainers to share their notes before leaving so that there is a combined feedback document.

Risk Assessment Walkthrough

- Provide Background and Prompt A, walk through an example of a risk assessment (such as protecting private information of staff member assuming harrasser(s) with limited technical skills/means, etc).

- Ideally, participants will be open to discussing their own organizations' circumstances. However, if there are any that are uncomfortable with that, there are additional prompts that are available that they can discuss in small groups instead.

- **Background:** Sheena runs a nonprofit organization helping connect low-income residents of City X with municipal services in their area. She and her 3 full time staff serve about two thousand clients annually. Currently, they collect information about their clients, such as name, address, income, health/medical needs, employment status, and family status, to find the appropriate services for their needs.

- **Prompt A:** Sheena's team has recently been in the news for their work, and after this publicity, they have been receiving threatening phone calls, in particular targeting their most public-facing staff member in charge of media relations. They have also received a few strange emails claiming to be from friends and former employers of this staff member.

- **Prompt B:** Sheena's team needs to add an intern to help them with outreach and fundraising, and wants to give this intern access to some but not all of their internal documents. Also, this intern will be using their own laptop and may sometimes work from home, since office space is tight and the team cannot afford to buy a dedicated work laptop for interns.

- **Prompt C:** Recently, Sheena had to fire one of her former staff members. This staff member had access to most of the accounts including the payroll/accounting software, online banking, and client records database.

Browsing and VPNs: Building definitions

Safe Browsing and VPNs Summary (with information on all topics– Facilitators keep this for answering questions, optionally hand out at the end.) In your group, discuss the following questions. Your goal is to build a 2-4 minute presentation for the larger group on the topic below.

The facilitators are here if you get stuck or have any questions!

Browser: What is a Browser? What browsers are we using? What are Browser settings for privacy and security? What is Private Browsing? What are trackers and cookies? What is anonymous browsing and when and why would you use it?

Network: What networks do you connect to? Who manages the networks you connect to? What do you know about them and their interests (starbucks, airport, your org)? What is visible to a network while you are using it to access the internet?

VPN: What is a VPN? When and why would you use a VPN? Who manages VPNs? What is visible when you're using a VPN – to your network, ISP, the services you are using, to your VPN? How do I choose a good VPN? How do I use a VPN? What are we already using and why?

Infrastructure: What is an ISP? Who runs ISPs? What information do they know about us and our internet activity? What is a National Gateway? Who controls these?

Workshop 2
FACILITATOR GUIDE

WORKSHOP 2: OUR WORK IS BOTH INDIVIDUAL AND COLLECTIVE

Data Stewardship and Security

Learning Objectives

- Our work is both individual and collective
- Determine what "data stewardship" means to us as individuals and organizations
- Understand risks to data privacy and security
- Gain understanding of data confidentiality and practices
- Deepen understanding of how networks and browsing work
- Gain familiarity with tactics and tools for network and browsing privacy and security
- Gain hands-on experience with VPNs
- Discuss motivation for increased browser privacy and security, and explore tools

3 hours

Activity	*Time (3 hours)*
Welcome: grounding check in, review commitments & agenda / Full group	***15 minutes***
Holistic Security Process / small breakouts	***30 minutes***
Building Power: Data Stewardship <speaker/presentation> / Small + Full group	***45 minutes***
Break	***10 minutes***
Tactics and Tools: How the internet works / Full group	***20 minutes***
Networks, Wifi, and VPNs / Small breakouts	***40 minutes***
Safe WiFi Access - VPN Demo / Full group	***10 minutes***
Closing: Homework, Resources, Announcements, Questions, Survey / Full	***10 minutes***

Prep and Materials

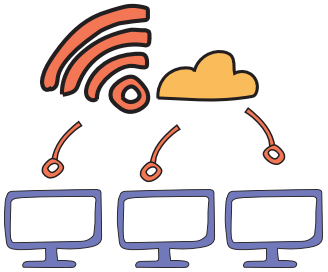
Print the following data security guides:

NYCLU - Fact Sheet (https://www.nyclu.org/en/know-your-rights/know-your-rights-five-ways-protect-against-cell-phone-spying)

Ways to Protect Your Cell Phone and Data
https://www.nyclu.org/sites/default/files/ecpa_onepager_20170308.pdf

Room set up needs:	Materials to print and prepare	Activities
Name tags, markers, Post its	List of Agreements	What we know (discussion)
Light snacks	Data legal handouts	Data my org collects (post-its)
Whiteboards or big paper	Internet Infrastructure cards	Presentation (handout or speaker)
Seating, set up in a circle, extra chairs if possible	VPN discussion prompts	Internet Structure (Matching Cards)
Projector	Homework handout	Browsing / Browsers (discussion)
	Evaluation	VPN demo (pre-load sites)

Internet Infrastructure: Card Term + Definition Matching Game



Also write or print the following on two cards:

- HTTP DATA
- HTTPS DATA

Browsers and VPNs > Activity For Participants

- PRINT one each of of the five "Building Definitions" sections on a page and hand out to five groups, or WRITE one section each on a poster and assign groups to be by the five posters.

Write on card
- Print definition

Wireless Network or WiFi
- a network that devices can join without being physically attached to its equipment

Wireless Router
- a device that connects computers on a local network (e.g., physical network set-up of the library) and links computers from the local network to the internet via an internet modem

Internet Modem
- connects to an Internet Service Provider (ISP), often via coaxial cable or ethernet cable, transmitting and transforming digital and electrical signals

Internet Service Provider (ISP)
- an organization or business that provides services for accessing the internet, e.g. Optimum, Verizon, Comcast

National Gateway
- physical infrastructure through which internet traffic leaves national boundaries

Web Host
- an organization that provides services for maintaining a website, including web servers

Web Server
- a computer technology that stores and makes data, such as web pages, available on the web

1. Welcome back/Re-establish shared space

15 min

Materials:

List of Commitments from last workshop

1.1 Welcoming and checking in

Facilitator notes: An icebreaker/gentle check in that involves going around the room. So that there is not an abrupt change from when people are arriving and when we begin the workshop, all facilitators, engage people in conversations as people arrive so we're already in conversation.

1.2 Review Learning Objectives, Agenda, Orientation to this space

1.3 Full group Review Collective Commitments (3 min)

2. Holistic Security Process – Small Group Work, Build relationships and Review Homework

30 min

The purpose of this section is to build trust between facilitators and participants so that participants can share how their processes and learning are proceeding and all can ask and offer what is needed.

Break into small groups 1 Facilitator + representatives from 2 organizations (if there is more than one representative from your organization, all reps join the group). Groups should be no more than 3-5 people. Facilitator lead these small group activities. Lead facilitator will call out time cues.

2.1 Small Group Relationship Building (15 min – everyone gets 3-5 minutes)

Goal: Everyone shares how they came to this work.

Facilitator Notes about how to frame the activity:

- **Framing –** let people know this is a space to bring yourself into professionally, personally, politically
- **Depth of sharing –** this may be outside of your comfort zone, please make this as personal as you are comfortable with and also you don't have to
- **Confidentiality –** this is a space for sharing and we keep each other's confidentiality
- **Guidelines about listening –** suggest people to listen and not to get into a back and forth; listen the whole time, hold questions or comments
- **Please don't plan while others are talking –** when it comes to you, you will know what is right
- **Affirmation and pause –** pause at the end of someone; take a moment to transition; say thank you, nod, eye contact; be consistent – respond similarly to each

Materials:

N/A

Ask - Answer the question: **what brought you to this work and what keeps you in it?** Share what motivates you personally, intellectually, politically, etc.

Ask to lead with your name, gender pronouns, identities that are important for you.

Time keep – There are x number of us. We have 15 minutes, we'll share it. We each have 3-5 minutes (based on the size of your group) to share and will share responsibility for success, in this case, share the role of keeping time. Ask people to keep time for the person before you. Ask someone to keep time for you and let you know gently when 30 seconds left.

Debrief – at the end, ask 1 question like, *how was that for you, process that and then, whatever comes next.

2.2 Small Group Share "What we Know About...": Risk Assessment, Password Managers and 2-Factor Authentication (20 min)

Part 1: Facilitators listen and facilitate full group discussion

Facilitator notes:

- The purpose of this section is to temperature check digital security knowledge, and name "what we're not talking about today".
- Facilitators take notes. (Request permission, privacy-conscious notes, not in Google Docs!).
- Identify one person from your small group to report back 1-3 things you are willing to bring back to the conversation.

Introduce these concepts: Risk Assessment, 2FA, Password Managers, Password Strength

Framework: Today we're focusing most on data security when we use web browsers, but we want to acknowledge there are many aspects to digital security. They get focused on in other workshops, but can anyone describe: Risk Assessment, 2FA, Password Managers, Password Strength (or use other concepts you think are important), or other ideas in digital security?

Detailed description: Share your experiences on any of the following activities: risk assessment discussions, evaluating password strength, choosing a password manager, setting up 2-factor authentication.

As the conversation continues, ask individuals from the small groups to summarize notes, and have a few points they are comfortable sharing. When the group comes back together, we will go around and share/summarize a point from each of our conversations.

Part 2: Group Debrief

The facilitator can then try to draw patterns, ask folks how they dealt with these challenges. Facilitators should note what comes up in conversation so that we can do a share-back at the end and not miss any points that don't get shared in the wider group.

Alternate framing - if this is a follow-up to an earlier workshop

Facilitator notes: If large groups > break out and have 1 Facilitator per discussion group. facilitate a quick discussion about any or all of the following topics: Risk Assessment, 2FA, Password Managers, Password Strength.

Say: This is a review. We introduced Risk Assessment, 2FA, Password Managers, Password Strength in Workshop 1.

Framework: Your homework was to do:

- a risk assessment on passwords and explore 2FA and Password Managers. What were: Challenges, Successes, Observations (a.k.a. Plus, Minus, Interesting) for you?
- *insert their other homework assignment(s) here*

In last 5 minutes, hold wider facilitated discussion tying topics/concerns together.

3. Building Political Power: Data Stewardship and Accountability (Guest speakers)

The purpose of this section is to introduce concepts of data collection and issues around legal discovery, legal processes through which your personal or organizational data may be accessed by government agencies or through legal proceedings.

45 min

Either invite guest speakers (what we did) or use the handouts to introduce ways that organizations can establish legal data stewardship policies to manage the reach of legal discovery. Participants will define data stewardship for themselves and begin to build understanding about how their organization can develop data policies in alignment with their sense of stewardship.

3.1 Data Stewardship: Defining our terms and our data (15 minutes).

Facilitator notes:

- brainstorming/popcorn-style.
- Facilitators try asking only questions here to arrive at shared definitions.
- You can break into small groups or stay full-group depending on how big the workshop participant group is. Ideally groups of about 5.
- Question-led discussions about what it means to be a steward/caretaker.
- This activity is designed to be participant led.
- Facilitators, facilitate conversations (by asking question prompts as us much as possible) and avoid lecturing.

Ask:

- What is stewardship, and what does stewardship mean to us? (~5 min)
- What is data, and what kind of data do our organizations collect and store? (~5 min)

Materials:

Post-its; Legal data handouts

Say:

These conversations may seem abstract at times but we hope to remain grounded in the realities of the communities we work with, which is why we've asked you all to think about the data the folks you work with have trusted you with. And so we have this list to remind us of why we're here and what we're working towards.

Next (10 minutes): Hand everyone a post it, ask them to write some data their org collects and then post it on a larger chart paper (helpful because it gets people moving because they have to walk up to post it and helps fight the post-lunch lag).

Then the facilitator can read out what people wrote (or ask for a volunteer to read out what people wrote).

Next (10 minutes): Hand everyone a post it, ask them to write some data their org collects and then post it on a larger chart paper (helpful because it gets people moving because they have to walk up to post it and helps fight the post-lunch lag). *Then the facilitator can read out what people wrote (or ask for a volunteer to read out what people wrote).*

3.2 Research + Learning: Legal Discovery and Legal Data Stewardship (20 minutes)

Materials:
- Copy out the terms in the exercise below onto cards, poster paper, or a whiteboard.
- Arrange ahead of time for the following materials to be printed.
- **NYCLU - Fact Sheet** on Electronic data privacy in NY state (if NYS is applicable) (https://www.nyclu.org/en/know-your-rights/know-your-rights-five-ways-protect-against-cell-phone-spying)
- **Ways to Protect Your Cell Phone and Data** https://www.nyclu.org/sites/default/files/ecpa_onepager_20170308.pdf

Facilitator notes: familiarize yourselves with the terms below and materials on the printed sheets ahead of time.

Instructions: In pairs, look up these term sets **(7 minutes):**

- PATRIOT Act
- National Security Letters

- Warrantless Wiretap
- FISA Court

- Grand Jury
- Legal Discovery

- PRISM
- Edward Snowden

When you look them up, ask:

- What do these have to do with access to our information?
- When was this invented?
- Do you know of or can you share examples of how this applies to recent movements?

Q&A (12 minutes - 2-3 per group)
Encourage people to bring their own organizational contexts in, if they don't already. Come back to large group and share definitions - Ask Questions

Break 10mins

4. Tactics and Tools: Networks and Wifi Access

Materials:

- **How the internet works** (cards) Matching definitions and infrastructure. Hand people these 8 cards numbered on the back (Computer, Wireless Network, Wireless Router, Internet Modem, ISP, National Gateway, Web Host & Server, Site)
- **Participant Handout:** Browsers VPNs (paper or pre-written on posters) there are 5 prompts, each page has a different prompt at the top, each group gets 1 to write on.

60 min

The purpose of this section is to deepen understanding of how data flows through the internet when we're doing common tasks like using web-based services and sending email. We will explore possibilities for making better decisions about how we're tools and services and what information we're giving up when we're using it. We will introduce privacy and security risks and then explore tactics and tools like VPNS and Browser privacy.

Activity: how the internet works - matching definitions and infrastructure (20 Min)

Part 1: Card Sort

Materials > see the In-Workshop Handouts & Activities section for print directions. Facilitator notes: This is deceptively short, but is thick participation and quite engaging.

If you have less than 16 people, place definitions around the room. Otherwise, hand each definition to 1 person (who is not going to get a Card).

Next, hand people the 8 Cards (Computer, Wireless Network, Wireless Router, Internet Modem, ISP, National Gateway, Web Host & Server, Site), ideally they are numbered on the back to match the definitions.

Ask participants to:

- find the definition that matches their card
- and then have them stand in order of operations
- Then, read out their definitions.

Here is the order: Computer, Wireless Network, Wireless Router, Internet Modem, ISP, National Gateway, Web Host & Server, Site

Next, they'll tie the whole flow together with….

Part 2: "Be the Data" As it Moves Through Internet Infrastructure

Facilitator: Facilitate participants describing an example of a person entering data to "surf" a simple HTTP and then a HTTPS site. Use the cards + definitions people are holding to follow data from entering the server request into a computer to the paths the request travels to return a web site to your computer. Explain what about the data is visible along the way by the element on the card it is "moving through" along the path it follows:

Again, here is the order the data follows: Computer, Wireless Network, Wireless Router, Internet Modem, ISP, National Gateway, Web Host & Server, Site

HTTP:
- Have the person at computer send a browser request for a website on a postcard that asks for a web page, TO www.nytimes, FROM my IP address.
- Pass this along through the internet
- When it's received by the site, attach the webpage and send back
- Explain that the request, the ip address, the returned content is all visible

HTTPS:
- Have the person at computer put a browser request for a website on a postcard inside of an envelope; the envelope on the outside reads TO www.nytimes and FROM IP address
- Pass this along through the internet
- When it's received by the site, the site opens the envelope, inserts the webpage and the request back into the envelope, and sends back
- Explain that the request to the site is visible, but none of the data; that the TO and FROM are visible.

Small group in-depth discussions: browsing, network, VPNs, internet control (20 min)

Materials > see the In-Workshop Handouts & Activities section for print directions for

Participant Handout: Browsers VPNs.
Split into 4 small groups, 1 facilitator per group.
Facilitators facilitate a conversation asking and answering each set of these questions.

Each group will tackle a set of questions from the Participant handout and prepare a 2-3 minute presentation of the topic that is physical or visual in some way (not just a spoken description). Presentations can be drawn posters, could use the postcard internet, could be group members representing concepts with their bodies. This is a different way to engage with information, that uses different parts of our intelligence and understanding.

Reportback (20 min – 3-5 min each group)

Each group presents the mini-presentation they prepared. Facilitators open the room for additions or questions after each presentation.

Activity: Hands on: Safe Wifi Access, A VPN demo (5 min)

Facilitator instructions:

Connect to wifi on computer that's connected to a projector.

Visit the website of the VPN provider you have chosen, and discuss a few points about why you chose them. Show the VPN app running on your computer, and visit https://dnsleaktest.com/ and run the extended test to show you are not leaking your DNS requests (check ahead of time!).

DNS leak test also has a page with a graphic explaining what a DNS leak is (tab called "What's a DNS leak?"). You can change your connection settings to another country/region and show that your IP address changes.

Question/Discussion (10 min)

Review: Facilitators, use these questions to wrap up and synthesize this section

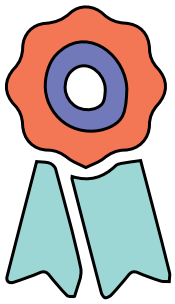
Discussion: What do we know about VPNs?

- Choosing a VPN
- Costs of using VPNs
- What VPNs don't protect us from (notes in handout)

Review

- Ask participants to popcorn
- Best practices while connecting to public networks and browser privacy

5. Homework, Last Announcements, Questions



Materials: Homework Handout, in the Participant Guide

Organizational reflection/taking inventory:

- Political - Conversation around data; potential of lean data practices for my organization
- Holistic - Onboarding and offboarding: what kind of procedures are in place?
- Hands on Tools - Data collection, use, flow, and protection; Choosing a VPN

If you're continuing to meet: Announce Upcoming workshop topics, and poll for new topics!

Time: Please try to leave at minimum 10 min (ideally 15-20 min) free at the end for open time: people are recommended to stay with questions/comments/concerns/chatting.

Workshop 3
FACILITATOR GUIDE

WORKSHOP 3: OUR WORK IS ABOUT LEARNING FROM AND TAKING CARE OF EACH OTHER.

Organizational Security as a Team + Topical Open Spaces

Learning Objectives

3 hours

- Our work is about learning from and taking care of each other
- Ground in the work of the organizations
- Support participants at different levels by providing possibilities for reviewing topics and tools or engaging with new topics and tools
- Policy and Organizational Change: Make connections between topics we have covered and participants using workshop material to develop organizational policies and organizational security
- Provide concrete takeaways for participants to reinforce and deepen understanding and practice

Activity	*Time (3 hours)*
Group Centering – Concentric Circles (full group)	***10 minutes***
Welcoming and Workshop Opening (full group)	***20 minutes***
Explain & Organize Open Space (full group)	***10 minutes***
Open Space I	***30 minutes***
Break	***10 minutes***
Open Space II	***30 minutes***
Open Space III	***30 minutes***
Break	***10 minutes***
Discussion on Organizational Security (full group)	***45 minutes***
Closing activity (Feedback, questions, next steps)	***20 minutes***
Announcements/Wrap	***5 minutes***

Prep Tasks & Materials

Open space

Assign facilitators or participant-experts to lead open space sessions:

Possible Topics

- Review Password Managers
- Review 2-factor authentication
- Review VPNs
- Alternatives to Skype (encrypted video calling)
- Review Secure Browsing
- Encrypted Messaging: using Signal or WhatsApp
- Filming / Documenting Safely
- Safer social media use
- Action Safety Planning
- Wildcard participant-led/requested

Print the following:

- Participant Guide - W3 (includes the Practices in Organizational Holistic Security: Preparedness Assessment handout)
- An evaluation - use the sample from the Evaluation chapter, or create your own.
- The Open Space topic facilitation sheets at the end of this chapter
- Org Security Phases (at the end of this Guide)

Room set up needs:	Materials to print and prepare	Activities
Name tags, markers, Post its	Write Collective Agreements & Agenda on a piece of large paper so participants can see	Open space sessions (x3)
Light snacks, coffee/tea	Homework / Workshop handout	Putting it Together: Organizational Security Process
Whiteboards or big paper	Evaluation	Presentation (handout or speaker)
Seating, set up in a circle, extra chairs if possible	Write out the Open Space topics you've chosen to offer in the workshop	
Projector		

1. Centering Activity – Concentric Circles

10 min

Materials:

N/A

Goal: Reconvene as a group, center the room on people in the room and their work:

Welcome folks in the room! Invite folks start the day in a large circle.

Make sure that participants are able to clearly see each other.

Ask folks to go around to: Have every other person take one step into the circle, turn around, and make sure you come face to face with another participant.

Then ask one question. Let them discuss, then have outside circle take one step to the Right or Left and ask another question.

- What's is one of your favorite media pieces and why?
- Share a practice that you use now that gives you strength?
- Share a moment that you have felt were successful in your work?
- What makes you present in this work today and how do you see this work empowering you both in your organization and in your life?

2. Welcome and Workshop Opening

15 min

Materials:

List of Commitments from last workshop

Name, Pronouns, and Org introductions, Weather Report

- Folks can share how they are feeling today (energy they are coming in with) as a weather report. This helps us gauge the energy in the room.

Review Goals & Agenda

- Acknowledging challenging moment in our community, we will hold space in this space if needed, but if folks are ok we'll move forward with our agenda.
- Reviewing collective commitments

3. Open Space: Explanation and Activity

What is it? Small groups facilitated by trainers

2 hours

Open space session:

Cycle 1 - 30 minutes
Break - 10 minutes
Cycle 2 - 30 minutes
Cycle 3 - 30 minutes

Goal: Orgs self-determine things they focus on, knowledge building, practice building, etc; specific tools/tactics sections
As a facilitator is explaining the open space (5 min), other facilitators can make sure the room is set up, and gently move handouts or writing materials as needed. If this is noisy, just wait til the explanation is over.

Roles needed: Timekeeper.

Setup: stations around the room with: large paper or whiteboard, markers/ writing materials, ample 'cheat sheet' handouts on current topic (1 per participant), 3-4 chairs, and facilitators 1-2 per station.

Explain: In the next activity, there will be breakout sessions on a variety of topics. There will be 1-4 participants per 1-2 facilitators and these sessions can be open-ended, from explanations, demos, deep-dives, or troubleshooting.

Participants are free to choose topics that interest them, or propose their own topic after they see the list if it is missing something. Participants may also want to lead or co-lead their own session, and this is encouraged in the 'Wildcard' slot.

Example Open Space Breakout map:
Depending on how many facilitators or participant-experts are leading open space sessions, you'll have the same or perhaps less options in each cycle.

Cycle 1	*Cycle 2*	*Cycle 3*
Review Password Managers	Review 2-factor authentication	Review VPNs
Wildcard participant-led/ requested	Wildcard participant-led/ requested	Wildcard participant-led/ requested
Alternatives to Skype (encrypted video calling)	Review Secure Browsing	Alternatives to Skype (encrypted video calling)
Encrypted Messaging: Using Signal or WhatsApp	Encrypted Messaging: using Signal or WhatsApp	Filming / Documenting Safely
Safer social media use	Action Safety Planning	Safer social media use

Break 10mins

4. Full group session – Putting it Together: Organizational Security Process

45 min

Goal: begin tying the tools and practices that we are learning for ourselves as individuals to the bigger picture of organizational security and developing processes.

Energizer + Transition (5 minutes - pick an activity to bring people together. Check the facilitators' guide section or bring in one you want to try.)

Discussion: Organizational Change – Pair Share
Ask participants to share stories about how their organization has implemented security policies and practices
Encourage people to share success stories and also stories of failure and correction

Hint: reach out to a few participants at break to ask them to be ready to be called on

Share the in-depth 1-1 Process we follow

Ground in the values of an organization
Discovery/Research

- **Team** - across an org, with a team of people who can lead the change. They have the authority, interest, time. A team that has breadth in the org (ie. one from each department)
- Do this with IT providers, IT managers, or operations and admin team
- **Risk Assessment** – work together to discuss risks of the work you are doing; risks to yourselves, to the people you work and organize with; discuss how people's identities and histories are linked to the risks they face; your organizational policies should be able to support your individuals who face varying levels of risks
- **Knowledge building** – making the case. Build knowledge about digital security risks, tools. Make this as participatory as possible so people can see their personal and professional digital use in this.
- **Political education** – make the case that some work is individual, some organizational, and some political.
- **Collaborative Policy Development** – Develop policies based on what the org is already doing. Make it iterative. Separate best practices from required policies.
- **Incident response team** – Develop a team of people who manage incidents, from Phishing email scams to arrests. Work to identify the types of incidents you might face, based on real examples. Develop a chain of action that is based on your strengths.

Deepening – read alone and discuss in pairs

- Pass out handout, have people read silently to themselves.
- PAIR discussion your peer from your org, a facilitator, another participant, and discuss these questions

Check out

- Facilitators frame this

5. Closing – Head, Heart, Hand

Goals: Close the space, discuss the trajectory of the workshops and invite feedback on how to improve.

Roles: One lead facilitator can open the conversation in this section, and the other can take notes. Feel free to switch roles partway through.

Conversation: In this section, we will close out the space that we shared today. Find a way to share the following 3 points with participants in your own words (approx 5 minutes), then use the remaining time (approx 15 minutes) to receive feedback from participants.

- **Arc of our workshops.** This workshop is in the midpoint of our 5-workshop series. The first two workshops have focused on individual tools and practices, as well as the political context that brings us into our work. In each workshop we explored a different format for sharing knowledge. The final two workshops will shift the focus to tools we can use as organizations. Beyond our workshops, there will be continuing opportunities for us to check in and broaden the skills and topics that we cover. These workshops are the beginning of a continuing process.

- **Gratitude for our pilot participants.** This project is a pilot, and we are still learning a lot about how to best serve our participants, what content to cover, and how we can improve the way we deliver this content and our workshops. We want to thank and acknowledge your effort and commitment to shaping this process with us—your feedback will help us shape the final months of this project and future versions of this program.

- **Your feedback shapes this program.** We want to open the floor for feedback about the content, the way we've delivered it, and what you've liked, disliked, or wanted to change. We've identified a few priorities: we're working to get more handouts, resources, and content available for your reference, and the end result will be a website with all content, facilitation materials available.

30 min

Final Wrap-Up (3 min)

Thank you for collecting this feedback. Thank participants for their time today, and ask if there are any announcements (Office hours, next location) for the next workshop before closing.

Open Space: Mini-Workshop Topic Support Sheets

The Resources section has 20 pages of 1-2 page mini-workshop resource sheets for participants; print enough so that you can pick it up if a topic is selected in open space.

The following pages have the *facilitation guides* for commonly-asked for open space sessions we offered a few times.

Alternatives to Skype Facilitation Notes:

Arc of the workshop:

Go-Around (4min)
Name, what brought you to this group, something you're looking forward to

Risk assessment/ what are you worried about (5-10)
What do you use video chatting for? How often do you use it?
Has your organization ever run into cyber attacks or infiltration? Court orders? Requests for data?

Agenda overview (1min)
Is there anything else you would like to discuss?

Activity exploring alternatives and their pros and cons [use handouts for these] (20min)

Create handouts with the logos + screenshot of the interface of these apps:

- Jitsi Meet, Appear.in, Wire, Skype and Google Hangouts. The back of the handouts will have a simple pros and cons chart. Participants will each receive one (this can be adjusted based on the number of participants), read the handout and then discuss with a partner. Guiding questions for their conversation:
- Compare the pros and cons of each app. What are similarities and differences you notice?
- Could either of these apps meet your/ your organization's needs? Why or why not?

Each handout will contain an expiration date. Explain what it means through these examples:

- AIM
- Blackberry

Debrief:

- Each person will present their app to the group and their impressions of it
- Did you learn anything that surprised you?
- Which of these apps do you think you might be able to use?
- What will be some of the difficulties when trying to bring it back to folks in your organization?

Shorten the above activity if there are other topics folks would like us to cover

Takeaways/ topics we'd like to cover in the discussion:

Risk assessment: if folks aren't sure why this is important

- Hate groups, nation state actors
- Different accesses, different capabilities

Assessing pros and cons of each of these options

- Think about the longevity of the project
- How secure are they? Biggest distinction: who is running them and what's their privacy policy.
- Just because they're not in the US doesn't mean they won't cooperate with our law enforcement services
- There isn't true end to end encrypted video chat
- Jitsi – security assessment – seem chill include in the Jitsi handout: we want folks to understand our methodology in evaluating which apps are and aren't secure
- Wire and Jitsi have extra protection between server and the client/ computer

Safe Browsing Facilitation Guide

Facilitation tip: Facilitators can print each question and hand one question to each participant. Give folks a minute to think about the question and their own practices. Then facilitate a larger conversation: What was your question and how did you answer it? What are you now thinking about? Why do you think this is important to consider?

When debriefing this, try to weave in the suggestions on adopting different internet usage habits that are below. It makes the suggestions more digestible if they're woven into the conversation. And after processing one question you can ask, "does anyone else want to share what their question was and how they answered it?" and then you can cover another suggestion.

Go Around: Your name, a one-word check-in and your concerns about browsing/ what brought you here

Opening discussion:

- What does safe browsing mean to you?
- Will someone share their definition of a browser?
- Browser: a software application that allows you to browse (retrieve and present) information specified by a URL (uniform resource locator). This information is generally on the web, but a browser can also be used to display or retrieve locally-found information or content. We use browsers like Firefox, Chrome, Safari, or TorBrowser to access and display websites.

Private Browsing

- Overview
- Activity

Instructions:

- So we're going to do an activity to talk about when a private browser may or may not be useful.
- You're going to take a post-it, write "True" on one, and "False" on the other.
- I'm going to read a statement, give you a few seconds to think and then ask you to raise the true or false card.
- Any questions? PAUSE
- A reminder: it's ok to be wrong, we're all in diff stages of learning about these things, no one is perfect. We're trying to think about things differently so it's not about being right or wrong.

Statements:

- If you want to protect yourself against malicious files or phishing, you should use a private browsing setting.
- *FALSE*
- *What should you use instead? Safe browsing/ downloading practices*
- If you want to log into Facebook or Gmail on a friend's computer but don't want to log them out of their account, you should use a private browser
- *TRUE*
- If you want to conduct sensitive research but don't want it traced back to yourself, you should do NOT use a private browser
- *TRUE*
- *What can you use instead? A VPN and/or Tor network*
- If want to stop a website from tracking you during a browsing session, you should use a private browsing setting
- *FALSE*
- *What can you use instead? Browser plugins that block trackers/ cookies (transition to next section)*

Trackers and Cookies

1. Overview - what ARE cookies?
2. Participatory Theatre of how third party trackers work

You're out hanging out with two of your friends

- John is there and you don't really talk to him, John's just there
- You're out there living your best life while John is just there
- When saying bye to folks, John goes for the shoulder pat
- But you don't realize that John put a tracker on you when he went for the goodbye shoulder pat
- And now John is all up in your business and knows where you go

What do you think of John?
What do you think John represents?

- THIRD PARTY TRACKERS
- When you visit a website, third-party trackers (cookies, web beacons, flash cookies, pixel tags, etc) also get stored on your computer.
- Trackers collect information about which websites you're visiting, as well as information about your devices.
- One tracker might be there to give the website owner insight into her website traffic, but the rest belong to companies whose primary goal is to build up a profile of who you are: how old you are, where you live, what you read, and what you're interested in. This information can then be packaged and sold to others: advertisers, other companies, or governments.
- Now Hadassah's going to talk about how to deal with John

Talking about Browser Add-ons:

Network Information, Safe Network Usage

Intro questions

- Who owns or manages the networks you connect to?
- What do you know about them and their interests?

Why does this matter?

- Using a network that you (or your organization) controls is different than using one controlled by another company or business. A network you don't know could be poorly configured, malicious, or have people (or devices) watching the traffic between your computer and the router. While browsing sites with https is helpful, there are still other kinds of attacks (for example, "man-in-the-middle"/MiTM attacks) that mean that the information you view and submit online is more vulnerable and visible on a network you don't control.

Activity and Debrief (both)

- To get ourselves thinking about safe network usage, we're going to hand each of you a question. Take a minute, and think about your answer. And then we'll have a larger conversation and ask you to share why you think these questions are worth considering.
- Larger convo:
- Does anyone want to share their question and how you answered it?

1. What are you now thinking about?
2. Why do you think this is important to consider?

- Try to weave in the suggestions

1. Does anyone else want to share their question and how they answered it?

VPN Breakout Facilitation Notes

1. Ask folksfor names and why are you in the VPN breakout?
2. Are you using a vpn?

Risk Assessment – why use a vpn

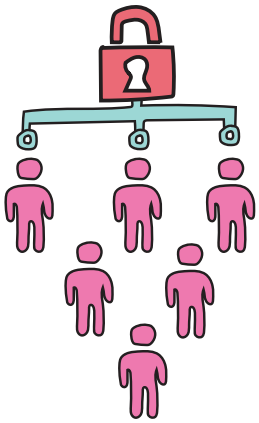
Anonymity & Privacy discussion

Choosing a VPN – Our shortlist and why

https://twitter.com/congressedits

Organizational Security:
Towards a Policy Development Process

Phase I:
Foundations
1. Vision and mission statement
2. Building a team
3. IT Operataions



Phase II:
Build Collective Awareness
1. Knowledge Building
2. Political Awareness
3. Risk Assesment
4. Team conversations: context, direction, value of our approach

Phase III:
Policy Development
1. Developing and revisiting policies
2. Incident response
3. Evaluate, update, revise

Phase IV:
Policy Development

WORKSHOP 4: WE DO OUR BEST WORK WHEN OUR VALUES AND PRACTICES ALIGN.

Policies & Procedures

Learning Objectives

3 hours

- We do our best work when our values and practices align.
- Guide organizational self-assessment of existing resources and practices
- Begin to articulate a stated security strategy/vision
- Hold discussions on policy building topics
- Dedicate time for individual security practices and 1:1 support
- Identify alignment or misalignment between values and practices, and work towards supporting practices that uphold our values

Activity	*Time (3 hours)*
Mind mapping (while people arrive)	***15 minutes***
Intro	***15 minutes***
Discussion: Aligning values with practices	***15 minutes***
Stretch & transition	***5 minutes***
Breakout sessions I: Policy development topic working groups	***55 minutes***
Break	***15 minutes***
Post food energizer	***5 minutes***
Strengths Inventory/skillshare	***30 minutes***
Stretch	***5 minutes***
Breakout sessions II: Policy development/how-to clinic	***45 minutes***
Next steps & Evaluations	***10 minutes***

Prep Tasks & Materials

Write out these using big paper or whiteboards:

- Agenda
- Workshop goals
- Community guidelines (maybe)
- Shareback options
- The different phases from homework for mind mapping exercise

Phase 1- Foundations: Ground Policies in the values of the organization & Build a Team
Phase 2 – Build Collective Awareness: Knowledge Building & Political Education
Phase 3 – Collaborative Policy Development & Develop an Incident Response Team

- Draw homework as a cycle
- Strengths inventory 3x posters: Campaigns/Actions, Strategies, Aspirations
- Parking Lot/ Garden

Print the following:
Print this chapter, including Handouts at the end

- Aligning Values and Practices Handout
- Intergenerational Working Group Handout
- Goals and Steps Handout

The participant handout found in the Participant Handbook: Workshop 4

Room set up needs:	Materials to print and prepare	Activities
Name tags, markers, Post its	Agreements / Community Guidelines	Review Mind mapping homework from Workshop 3
Snacks and coffee/tea? (Make a plan if you want these)	Homework / Workshop handout	Group Discussion: Aligning Cultural and Digital Practices
Whiteboards or big paper	Evaluation	Policy development working groups
Seating, set up in a circle	Agenda and Goals	Strengths Inventory Skillshare
Extra chairs		Optional how-to clinic
Projector		

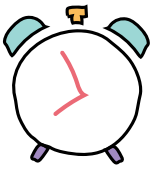
Workshop 4
FACILITATOR GUIDE

1. Mind-mapping while folks are trickling in (0:15)

Goal: Reconvene as a group, center the room on people in the room and their work:

Mind-mapping exercise with each of the phases from the homework. Participants will walk around and write their thoughts on each phase of the homework. They can write down whatever comes to mind – questions, reflections, thoughts on implementation. Participants can respond to what others have written as well as share their own thoughts. Encourage them to go back and read what others write and continue adding to it throughout the day during breaks.

2. Checking in/orienting to space



15 min

Welcome back! Leads decide on a short icebreaker as folks enter the space.

- Icebreaker
- Agenda Overview
- Intro
- Reviewing community standards
- Remind folks about the mind mapping

Detailed Intro:

- This workshop marks the turning point from focusing on our skills as individuals to fostering the development of these skills in the ecosystem of our organizations.
- We have been exploring tools and tactics we can use as individuals or groups to protect our privacy,
- Next step: build out knowledge we hold into organizational policies
- Policy work may seem anticlimactic it's part of creating resilient secure systems.
- Without policies:
- we have to rethink and revisit every decision to make sure it adheres with our values or vision.
- we run the risk of handling situations with contextual bias, or without proper resources,

Materials:

- 3 pieces of paper with the homework topics on the top, per the prep work.
- Post-its
- Markers

- we lose the robustness and integrity of the strategies we have been putting in place to protect ourselves
- The rest of our curriculum is about drafting policies rooted in our needs and vision
- We're all in process; no shame; no pedestals

Facilitator: Acknowledge the homework
Let's look back at the map we received as homework. It is divided into 3 'phases'—a grounding phase, a building/assessment phase, a policy-drafting phase—and it's iterative, meaning that for meaningful, healthy organizational policies, we will have to revisit steps of this process repeatedly. We won't go over it explicitly, but we hope it will guide the entire workshop today and that you can keep it in mind as we go along.

Suggested script - Self-assessment: Where do you see your organization in this process? Most of us may be working through Phase I or II for the first time. Some of us may also be working through Phase 0–prepare yourself with your own individual tools and tactics. There is space to work on all of those levels in this workshop, as well as in the coming weeks.

15 min

3. Building Political Power: How mission and values shape our policies

Group Discussion: Aligning Cultural and Digital Practices

Facilitator materials: Aligning Values and Practices Handout (end of this document)

Facilitator notes: We can go through the example in the handout, and participants can take this back to their own organizations to draw the link between values and practices.

Let's avoid voicing criticism for existing practices ("don't share passwords"), instead trying to look at positive/additive strategies ("have secure logins for each individual").

Facilitator materials:

Aligning Values and Practices Handout (end of this document)

Intro: What does alignment between our values and our practices look like?

- Based on reading **"Practices in Organizational Holistic Security - Preparedness Assessment"** - in your Resources chapter
- Getting us to think about how our values and expectations as an org and our practices (digital and physical) align or diverge
- Doesn't matter where we are in the policy development process – there's always space to reflect on whether current policies and procedures reflect our values and goals

We'll break up into groups of 3

- Give you a scenario
- It'll touch on differences between cultural and digital practices
- Then we'll come back as a group
- Let's avoid voicing criticism for existing practices ("don't share passwords"), instead trying to look at positive/additive strategies ("have secure logins for each individual").

Debrief

Explain What's Next (2 min)

Announce that we're stretching then doing breakout sessions.

Transition (0:05)

- Stretching then breakout sessions.

Facilitators: set up room for breakout sessions

Breakout Sessions: Policy development working groups (55 min, includes small groups and shareback)

In this section, we will choose an area of interest and conduct a breakout session.

Our goal is to have a conversation and create some content to share back with the larger group **(2-4 minutes)** at the end.

Options for sharing back include:
A presentation of the key strategies, points, or solutions that were discussed; a pictorial representation (flowchart, diagram, etc); a human sculpture; a one-page summary, a checklist/worksheet for others to use in the future; a written summary, etc.

Working Groups (40 min)

Topics we can choose from include:
- Identifying short-term, medium-term, and long-term goals*
- Assessing physical security at the office
- Disrupting existing workflows
- Addressing intergenerational issues when taking these practices and tools back to your organization*
- Wildcard topics tbd
- * = has handout

Facilitator notes: With 10 minutes left in the working groups, remind groups of the time left and prompt them to decide how they'll share back the information to the greater group.

55 min

Shareback (15 min)

In small groups, participants have 2-4 minutes to present their work to the larger group.

Facilitator notes: encourage participants to choose a shareback option (even if there's a dead silence when you ask, let the silence simmer!).
- Close out & let people know we have a 15-20 min break.

Break (0:15)

Energizer (0:05)

- Hand out the cards (make sure we have an even amount of people)
- Everyone's received a card with a name of an animal. I'm going to ask everyone to really get into character by making the sound of your animal, moving like your animal.
- Everyone has a partner who is the same animal you are and you're goal is to find them.
- But you're not allowed to speak to anyone so no conversations. You need to find them based on their sounds and body language.
- Once you find your partner, take a seat next to them.

Strengths Inventory: Skillshare (0:30 minutes)

Facilitator notes: One facilitator set up 3 big pieces of paper/3 columns on a large whiteboard for: Campaigns/Actions, Strategies, Aspirations (for debrief)
Intro & Directions (5 mins)

- Policy work can sound overwhelming
- So we're going to take time to contextualize it within work you've already done and successes you've had
- We're going to be thinking about existing strengths and practices that your organizations have adopted

Directions: Pair Share (15 mins)

- Find your partner from the energizer who was the same animal you were
- I'll read a question, you'll each take 2 minutes to answer it. Whoever goes first has the full two minutes and they can fill that space however they'd like. If you're answer doesn't take 2 full minutes and you'd like to fill the space with silence, that's fine.
- I'll let you know when two minutes is up
- The question is: What are resilient practices you've encouraged members or clients to adopt in their lives?
- Whoever was louder when making animal noises goes first
- Find another partner, someone who you haven't spoken to today
- What have been some areas that you've succeeded in making change in your organization?
- Whoever has longer hair will go first
- Find your last and final partner, someone who you do not know
- How do you build knowledge in your organization or community?
- The person with the lighter color shirt goes first

Debrief (10 mins)

- Does anyone want to share something they shared with their partner? Any other stories of success?

One facilitator will scribe while the other will take input from participants. Feel free to switch roles partway through.

The following are some prompts to begin the discussion. **You don't have to use all three prompts!** The goal is to start a conversation and welcome whatever direction the feedback takes. We are looking at ways that we have each been successful and sharing that back to each other as a group.

When something comes up, try to include it in one of the above categories

- Campaigns/Actions–for examples of specific things that went well
- Strategies—for examples of general tips that have been successful
- Aspirations—for if/when folks list things they want to try instead of things that have happened.

Facilitators: Start with the first prompt, and wait for a response. If the conversation fizzles out after a few attempts and/or reaches a natural conclusion, you can use the other prompt(s) at your discretion, or come up with new ones.

- What are resilient practices you've encouraged members/clients to adopt in their lives?
- What have been some areas that we have succeeded in making change in our organizations?
- How are we building knowledge in our organization or community?

Finally, if people are struggling to volunteer things they have already done, or if there is time at the end, you can ask,

- Based on our work today, what is one aspiration you have for creating change in your organization?

Stretch Break + Energizer (15 min)

Breakout Groups II: Policy OR optional how-to clinic (45 min including small group and shareback)

Overview:

- We're doing another round of breakout groups but switching things up this time
- For those of you who want to continue to talk about policy groundwork, we have options
- But for those of you who want to focus on specific skills or tools you can opt for a 1 on 1 clinic.
- We'll start with 1 on 1 clinic options and then I'll ask the facilitators to share what their breakout groups are about

Small groups & Clinics (30 minutes)

- "Are you sure you're not paranoid?" How to respond and conduct a risk assessment grounded in your community's history* (has handout)
- Choosing Alternative Tools (has handout)
- Phishing + email hygiene
- Clinic: 1:1 support with: Password Managers, 2FA, setting up a VPN, Signal + comms, examining risk assessment scenarios, or any of the topics we have covered already
- Wildcard topic TBD as participants ask for

Note: At 10 minutes left, walk around and let folks know they have 10 minutes left.

Shareback (15 minutes)

Facilitators, invite the group to thank everyone for sharing, especially participants who do one-on-one clinic work and are comfortable sharing what they were working on.

Everyone stands up in a circle, we throw around a ball and when they catch the ball each person shares something they learned from their session. It can be something you'll take back to your organization or something you're thinking about.

45 min

Next Steps (10 min)

Announcements.

- Next month's workshop is our last session together.
- [If applicable] Fill out the evaluation forms, take your time giving us feedback so we can tailor the next workshop to fill your needs.

Homework

Drafting Organizational Policy Breakout Session Topics

To help structure these sessions, you use the following prompts to get you started:

- What is something about this topic you're struggling with?
- What is one thing about this topic that you're doing well, or are proud of?
- What is one thing about this topic that you'd like to be able to talk about together?

Breakout I

Goal-setting: Identifying manageable short-term, medium-term, and long-term security goals
What are the factors that go into determining if a goal is short-term, medium-term, or long-term? Come up with some goals you may have for your organization(s), and explain some tactics the group can use to determine how to forecast their goals.

Assessing physical security at the office
Discuss your physical security at work, and/or any measures you have taken or would like to take to address physical security concerns. If you have gone through a physical security assessment, include which elements of this assessment did or did not feel helpful.

Disrupting existing workflows: Creating buy-in, addressing the transitions while adopting new practices
A working group to address the issue: "how do I get people on board?" Often when we adopt or suggest new practices, we cause disruption to existing workflows. What are some ways to honour and address that while still moving towards more secure digital strategies? What has worked, what hasn't?

Addressing intergenerational or technical proficiency gaps when taking practices and tools back to your organization
We have received a lot of feedback that sometimes, adopting new practices can divide the team along lines (senior vs new staff, different work styles, different generations). We will collaboratively address ways to handle gaps in adopting practices and how to include all team members in tool, tactic, and practice adoption.

Wildcard: TBD!
What are we missing? Create your own session(s) around any topic you feel engaged in. Please find a way to share back your findings with the group!

Breakout II topics

"Are you sure you're not paranoid?" Conducting risk assessments grounded in your community's history
Sharing responses to these and other challenging questions, and producing an example risk assessment, risk assessment template, or other piece that grounds our work in realities relevant to our communities.

Choosing Alternative Tools
What are the ways we evaluate and choose alternatives to some of our most ubiquitous tools, such as G Suite/Google, Skype, text messaging, or Dropbox? Based on our work so far, discuss strategies that you use to decide if a tool may meet your needs as an organization, and share how you might facilitate a switch from one tool to another. You can produce a step-by-step instruction set, a short play/skit, or host a Q&A with the group—feel free to be creative.

Phishing Training
Discussion on avoiding phishing attacks, compiling a list of strategies to build a digital culture where phishing attacks stick out and raise suspicion, and resourcing each other on what to look for (or what to avoid).

Wildcard TBD!
What are we missing? Create your own session(s) around any topic you feel engaged in. Please find a way to share back your findings with the group!

Activity Worksheet: Aligning Values and Practices

Adapted from Cultural and Digital Security Practices by Kyla Massey

In our organization, our cultural practices are the practices, routines, and activities that we engage in. Whether deliberately created (for example, a practice of having staff meetings every Tuesday) or emergent (such as the observation that all staff always walk to the metro in pairs when leaving after hours), we have practices that become norms at our organization and affect our culture there as a team.

We also have such practices around our digital selves—for example, keeping the wifi password posted on a sticky-note on the fridge, or shredding old files once a month—but we often don't explicitly recognize these as practices that also create their own norms.

It is our goal to make sure that our practices (both cultural and digital) align with our values and mission as an organization.

Consider the following example.

Given the description below, identify at least 1 cultural practices and 1 digital practices of this organization, and indicate whether they align with the organization's goals.

This 15-person nonprofit organization, End Youth Homelessness, has the following mission statement: "Remove systemic barriers and stigma, and advocate for low-cost housing for youth facing homelessness."
In their work with advocating for low-income and at-risk clients, they collect Social Security numbers, credit reports and other financial information. They also have clients' contact information, including email addresses and phone numbers.

EYH's office building has a front desk check-in, where ID and sign-in are required. EYH employees have their own work laptops, which they mostly leave at the office overnight. They have a shared Twitter and Facebook account to which everyone on the outreach team has access. EYH stores client data both onsite (on a hard drive) and in the cloud—they have an encrypted client database that is maintained by a contracted 3rd party company.

Talking to the EYH team, you find out that their security goals are: protecting client and employee data, and making sure that their client list stays private within the organization to avoid any potential stigma associated with using their services.

- **A cultural practice they have is:**
- **A digital practice they have is:**
- **Does the practice align with their organization's values and/or goals?**
- **If you feel that they do not align, can you discuss as a group some ways that they could bring their practices into alignment?**

Intergenerational Working Group Handout

Key Question: How can we address intergenerational and/or technical proficiency gaps when bringing privacy practices and tools back to your organization?

It's important to consider that when exploring new tools and tactics to strengthen privacy practices in our work, it is equally important to identify challenges our communities might face when adopting these new protocols into their day to day. Moving forward with one strategy to onboard protocols may not apply to varied experiences in your community, which could be isolating and divide the team along lines (ex. senior and new staff, work styles, generational gaps, technical proficiencies etc.)

In our working group, we'll collaboratively explore ways to address these gaps, reflecting on practices we already use in our work. Our goal is to have a conversation and create some content to share back with the larger group (2-4 minutes) at the end.

Guiding Questions

- What are the potential challenges that your community may face in collectively adopting new privacy practices? What gaps need to be bridged?
- How would addressing these gaps help apply new protocols to your organization/with your community members? What would be the outcomes?
- What are some practices and tools that you already use in your work that could support this process? What could be a new approach you can use?

Let's take the last 10 minutes to decide how we'll share back our conversations to the larger group. Options for sharing back include:

- A performance or roleplay;
- a presentation of the key strategies, points, or solutions that were discussed:
- a human sculpture, artistic representation, pictorial;
- a one-pager/worksheet others could use in their work etc.

Goals & Steps Handout

How to Create and Prioritize Goals + Steps So You Can Do Them!

Approach: Tactical + practical analysis to identify the parts of a concern that you can address.

1. Name the issues or things you're concerned with, using what you've learned and what is already flagged for you from your team, boss, general concerns or observations.

- These are the WHY of your goals.
- Rank them in order of priority (from risk assessment). Note that not every issue is going to be addressed, and that's ok.

2. Rewrite the "issue" as an outcome to name it as you would a goal:

- Try flipping the description from negative to positive: For example goal for: "I'm worried about site getting hacked" = "Research two ways to secure our site."

3. List out things to do for the goals in order

- Important: Choose what you can do FROM your current situation, today
- How small of a piece can you make it into? Something you can do in 30 minutes is ideal, since you can do it tomorrow :)
- For example a task for "I'm worried about getting hacked" = "Set up SSL for site"

4. Determine short, medium, or long term status given priority AND complexity of tasks

What are the goals inside my issues? What's their importance? What do I need to do next?

ISSUE OF THE PROBLEM	PRIORITY	GOAL NAME	TASKS TO DO	SHORT, MEDIUM OR LONG TERM?
(example) All my passwords are all over the palce and I know I'm supposed to be in a password manager	(example) 10	(example) Set up a password manager	1. Ask 2 trusted friends what password manager they use, the price, and complexity. 2. Decide on the password manager I want. 3. Sign up for the account and enter my email account passwords. 4. Set time on my calendar to put this on my phone.	
			1. 2. 3.	
			1. 2. 3.	
			1. 2. 3.	

Working Group Handout: Are you Sure You're Not Paranoid?

Alternatives to Google Apps

Policy Development Working Groups & Share Out

Working Group Topic: "Are you sure you're not paranoid?" Conducting risk assessments grounded in your community's history.

In our working group, we'll collective share/brainstorm responses to these and other challenging questions producing an example risk assessment, risk assessment template, or other piece that grounds our work in realities relevant to our communities.

SAMPLE RISK ASSESSMENT: Staff Digital Communications

Work Area

- Do you use a work computer for work?
- Is your work computer encrypted?
- Do you use a personal computer for work?
- Is your personal computer encrypted?
- Do you access work email on your phone?
- Do you access work files on your phone?
- Do you use any security practices on your phone?
- What Wifi do you use for work? Home, office, cafe, etc.

Using revised risk assessment to build our messaging.

Use the below guiding questions:

- How could we use this tool to respond to these questions? What is the message that we want to convey?
- Who are you telling this message to and what is the intended impact?
- What is the best platform to communicate with your primary audience?
- What other tools can we use to do that create and deliver our message?

Functionality we want to replicate that Google Drive and Dropbox provides

Alternative tools	Collaborate in real time	Sharing	Access control & permissions	Mobile optimized	File storage and hosting	Notes on these tools
OwnCloud	x	x	x	x	x	• Need to install and self host on a server
NextCloud	x	x	x	x	x	• Need to install and self host on a server
Mayfirst server	x	x	x	x	x	• Affordable for nonprofits - but not free • Need to use a server • Will fight the FBI/law enforcement for you
TresorIt	x	x	x	x	x	• Secure cloud storage hackers really like
SpiderOak	x	x	x	x	x	• Secure cloud storage hackers really like
Pirate Pads, Ether Pads, RiseUp Pads	x	x	x	x	x	• Online. After 30 days your file goes away
LibreOffice	x	x	x	x	x	• Need to install and self host on a server
LibreOffice	x	x	x	x	x	• Offline space (a physical drive or USB

Why use alternatives to proprietary (corporate) software?

- Google spends billions of dollars to normalize Drive and make it really easy to use… for a reason.
- A corporation owns - and may benefit from - the content and data we put into Google Drive, Dropbox, Skype
- Content we put "in the cloud" can be sapinaed and most corporations will share it
- Accidents happen with permissions
- Google Machine-reads the content we put in
- Sheets is NOT excel and Docs is NOT word (or InDesign)

YOU CAN NOT PUT SENSITIVE CONTACT OR FINANCIAL INFO INTO DRIVE OR DROPBOX SAFELY

Workshop 5
FACILITATOR GUIDE

WORKSHOP 5: OUR WORK IS ONGOING, AND THIS IS THE JUST START OF A LONGER, SUSTAINABLE PROCESS.

Incident Response Strategies & Series Wrap-up

Learning Objectives

3:40 hours

- Our work is ongoing and part of a longer, sustainable process
- Understanding cultural shift that needs to happen, not holding this on one's own shoulders alone, how to rally our teams to this work
- Do a deep dive on encryption, backups, choosing tools and safer social media practices
- Learning how to respond to incidents and maintain organizational security in a crisis situation
- Reflecting on individual transformation as well as organizational changes throughout the course of the workshop series

Activity	*Time (3:40 hours)*
Opening Activity / Energizer	***15 minutes***
Intro Session	***15 minutes***
Breakout Sessions	***40 minutes***
Group Share Back	***15 minutes***
Break	***15 minutes***
Incident Response In Teams	***40 minutes***
Incident Response Presentations + General Debrief	***20 minutes***
Food Break	***15 minutes***
Community Driven Energizer (stretching, movement)	***5 minutes***
Group Timeline of Ground we've covered	***20 minutes***
Survey	***15 minutes***
Web of Support / Certificates / Appreciation and Closing Comments	***15 minutes***

Prep Tasks & Materials

Write out these using big paper or whiteboards:

Print the following:

This document, including the materials at the end
- Breakout Session descriptions
- Incident Response Guide
- Past workshop cheat sheet
- The Participant handout
- The Survey for final evaluation (if you're using a print version)

Room set up	Materials to prepare	Activities
Name tags, markers, Post its	List of Agreements	Open Space Breakouts
Light snacks, coffee/tea	Participant workshop handout	Incident Response Runthrough
Whiteboards or big paper	Incident Response Guide	Group Timeline
Seating, set up in a circle	Posters - 1 for each past workshop	Web of Support
Extra chairs (if possible)	Final evaluation survey (print or digital)	

Participants Arrive (10 min)

Facilitators encourage folks to get settled.

Opening Activity / Energizer (15 min)

Facilitators, let's open the space with an activity that people can join as they walk in. Maybe it is sharing something they did this week that they are working on, or doing a rose/bud/thorn (something positive, something potentially growing/new, something challenging).

Intro Session (15 min)

Goals: ideally, energizer at top of session should transition to the goals for today's session.

- Understanding cultural shift that needs to happen, not holding this on one's own shoulders alone, how to rally our teams to this work
- Do a deep dive on encryption, backups, choosing tools and safer social media practices
- Learning how to respond to incidents and maintain organizational security in a crisis situation
- Reflecting on individual transformation as well as organizational changes throughout the course of the workshop series

Agenda Overview & Reviewing Community Norms

Breakout Sessions (40 min)

Setup: For this part of the day, we're following similar format from the last session. We'll be going into a deep dive on particular themes related to digital security. Our goal is to develop collective knowledge to build and contribute tools, strategies, analysis, and practice across the group. Remember that there's a deep dive into each of these topics in your Resources as well..

Process: Participants will choose from 4 topics. You'll have 45 minutes to discuss the topic and work with your group. Participants should hold discussions with a mind towards creating something to share back with the group (2-4 min) at the end, whether it's a document, skit or enactment, drawing, checklist, or presentation. Have facilitators positioned around the room introduce the topic they will be supporting in conversations.

Topics:

- Encryption
- Backups
- Choosing Tools
- Safer Social Media

Detailed topic descriptions can be found further along in this chapter.

Lead facilitators will announce the final 10 minute marker, which means your group should gather thoughts and content on what you'd like to share back with the larger group.

Group Share Back (15 min)

2-4 minutes per group, with questions from other participants after each presentation.

Break (5 min)

Bathroom break, grab some more coffee and snacks! Facilitators Setup for Incident Response Activity: 2 stations with chairs in circle, writing materials (pen/paper/whiteboard etc) at each.

Incident Response In Teams (40 min)

Materials: see previous setup instructions, plus 2 scenario cards (1/2-page handouts or cards with the scenario printed).

Intro: In this activity we will draw on all of our knowledge, as well as the knowledge of our group members in order to come up with a plan of action for responding to an incident. Working in two different teams, members will discuss a scenario and come up with an incident response plan.

Content Note - Please discuss: Doing an incident response can be an intense experience for some folks, especially if the scenario hits close to home. Everyone is free to participate as much or as little as they are comfortable, and to take some space outside the room if they need. Our classroom commitments include that this space is for everyone to learn however they need, and also that what happens here, stays here. If anyone has any concerns or questions, they can talk to (name a facilitator or volunteer)

Introducing Scenarios: You may want to conduct an abbreviated risk assessment and/ or take some time to discuss the scenario and your team's understanding of it before you begin planning. You will have 40 minutes to discuss and develop your plan, which can take many forms, including actions, meetings, software use, tools or tactics that we've learned, or other interventions that you might use in your own work.

Guiding Questions for your teams

- What's the first step? What are some tools and tactics you could use?
- What are long and short term actions the org should take?
- What are potential barriers to implementing these action items?

Teams will have 5-10 minutes to present to each other at the end of this process, and then we will have a debrief period. Incident scenario at end of doc.

Teams can only ask facilitators 2 questions for guidance during this activity – it's like a gameshow. Assign point people for the teams to ask their questions to.

Incident Response Presentations (10min) + General Debrief (10 min)

Each group presents (approx 5-10 minutes per group) outlining their analysis of the situation and the steps they would take. After each group has presented, facilitators can ask the groups questions. Then we'll open up the remaining time for general debrief.

- What parts of this process were challenging?
- What kinds of questions arose for your group?
- How did you decide what to prioritise?
- How do folks feel after having done these scenarios?
- How do we get our team involved in this and work with them to think this way as well?

Snack Break (15 min)

Facilitators: we are moving back into whole group work, so please ungroup chairs etc as needed during this break.

Community Driven Energizer (5 min – stretching, movement)

Let's get one of our participants to get our bodies moving. Have participants facilitate energizer.

Timeline of Ground we've covered as a Group (20 min)

A recap: some ground we've covered over the past 5 months.
Facilitators, we will setup chart paper around the room. There will be four pieces of chart paper spread out across the room to recap the concepts and tools/tactics we covered in each workshop. *(see end of this chapter for a list of stated goals of each past workshop to put on the chart paper)*

We will ask for one facilitator to stand by each workshop and talk for 2 minutes about what was covered in that workshop. You can start with a quick recap (which will be on the chart paper) and then ask participants to expand on the general ideas that will be on the chart paper and to recall what they remember from the workshop (which will likely be nothing since some of this was months ago so please prep a question to help jog people's memory). Facilitators will remain at the same workshop for the whole activity (see list below), and after 2 minutes participants will go onto the next group to discuss a different workshop.

After each participant has had a conversation about each of the 4 previous workshops, we will as participants to reflect. In between each of the chart papers for Workshop 1 & 2, and Workshop 3 & 4.

We will have a chart paper split into two categories: Individual and Organizational. We will ask participants to write down reflections: what they learned, what they were thinking about, what they tried using/implementing in between each of the workshops. We'd like them to think about what they did as an individual, and what they did within their organization. **Participants will have 5 minutes to walk around and write their reflections (on sticky notes and then post them).**

Then we'll regroup and do a 5-min debrief thinking about the series of workshops more holistically so participants can reflect, share feedback and what worked and what didn't.

We'd like to ask you how it went.

Facilitators: hand out metrics surveys/documents.

Survey time (15 min -> when done, free to move to stretching/snacks!)

Facilitators: encourage folks to quietly get up, grab snacks, stretch etc when done with feedback surveys.

See the Evaluation Chapter for a sample Exit Survey

Web of Support / Appreciation, Certificates, Closing Comments (15 min)

This activity is meant to celebrate the connection and community built in this space. We all know that our learning and growth doesn't end here. We want to look to the community and network we've built to continue a network of support and learning.

Activity:

Participants and facilitators get into a large circle,
Facilitator starts, prompt everyone in the circle to think of something they would like to seek support on past this workshop,
If there is someone in the room that feels that they can support, the yarn will be thrown to them,
That person can share how they can support and then ask for support themselves.

CLOSING REFLECTION

What is one thing we are glad we learned, one thing that's next, and one piece of advice either for us (facilitators) or cohort (participants)?

We will end going around and sharing our thoughts as a way to close out this workshop.

Q&A + snacks! (til end)

Workshop 5: Printable Support Materials

DETAILED TOPIC DESCRIPTIONS for Breakout Sessions - print for facilitators

Encryption: We have talked about encrypted chat and video applications like Signal, WhatsApp, and Jitsi, and have touched on encrypting our phones and SIM cards in office hours.

Now we will discuss a crucial element of security: file and disk encryption. Learn what encryption is, discuss different options for file or disk encryption, and understand how you could set up encryption on your own device(s).

Backups: Security and privacy are important, but so is availability--the idea that you can access your data when you need it, and you know it will be there.

Having regular, secure backups in the event of emergency, theft, simple hardware failure, or other circumstances are important for keeping you and your organization from being thrown off course.

Choosing Tools: How do we choose new tools once we have decided we need them? We go through a process, similar to risk assessment, of evaluating our needs and the options and drawbacks of many possible solutions.

In this case, we will work together on what makes a reliable, reputable, or usable tool, how to research tools, and how to determine whether a new tool (of any type) meets our needs.

Safer Social Media: Social media platforms are a part of all of our activism.

Social media use is not an all-or-nothing decision; as activists, there are still ways we can use social media platforms like Twitter and Facebook while still being mindful of our privacy needs, as long as we understand what those platforms are doing and what kind of data they collect. We will facilitate a deeper dive on social media platforms.

(print the following page for each group you expect will be doing an incident response run-through)

Incident Response Scenario

CONTEXT

You work at a six-to-ten-person nonprofit with a larger (~10-20 person) volunteer staff who work. Your organization helps people sign up for and access city services and advocates, organizes community events, and sometimes provides assistance or interventions on their behalf. Many of your clients are undocumented, and others have friends or family who are undocumented.

TECH

Your core staff works out of a central office, and your volunteers work both from the office and remotely, on their own laptops. In order to provide your services, you have a database of clients, which includes their names, addresses, and a contact method, as well as the type of service they are receiving through your organization. The database can be accessed online by all core staff and by certain more long-term volunteers.

SCENARIO

You are summoned to an emergency staff meeting where you are informed that a portion of your database appears to have been leaked on pastebin or a pastebin-like site.

YOUR RESPONSE?

What steps do you take, both on an immediate and/or on a long term level?

You are free to include or add details about the situation, and please be prepared to discuss your reasoning/thought process around some steps you might take.

Cheat Sheet for Timeline - Workshop Key Takeaways

Use the objectives of the past workshops below to create reminders and keywords on your posters for the Timeline activity.

Wkshp 1 - In this workshop, participants will:

- Build a shared understanding of how politics and power shape the technologies and practices of surveillance
- Discuss and share strategies for using collective action to shift the design of technologies and practices of surveillance
- Understand shared experiences and shared challenges/opportunities
- Develop risk assessment as a tool to bring back to each organization
- Build knowledge about reducing unauthorized access by using strong passwords, password managers, and 2FA as tools and tactics to bring back to each organization
- Understand how to use 2-factor authentication and storing backup codes
- Understand how to use a password manager
- Recognize phishing attacks and identify ways to change phishing-vulnerable behavior (if time)

Wkshp 2 - Learning Objectives

- Determine what data stewardship means to us as individuals and organizations
- Understand risks legal discovery poses to data privacy and security
- Gain understanding of data confidentiality and practices in other industries
- Deepen understanding of how networks and browsing work
- Gain familiarity with tactics and tools for network and browsing privacy and security
- Gain hands-on experience with VPNs
- Discuss motivation for increased browser privacy and security, and explore available tools
- Begin to map access privileges and identify procedures during on- and off-boarding of staff

Wkshp 3 - Goals of this workshop

- Re-ground in the work of the organizations
- Support participants at different levels by providing possibilities for reviewing topics and tools or engaging with new topics and tools
- Policy and Organizational Change: Make connections between topics we have covered and participants using workshop material to develop organizational policies and organizational security
- Provide concrete takeaways for participants to reinforce and deepen understanding and practice
- VPN training #2
- Safe Browsing
- Alternatives to Skype
- Alternatives to Google Docs

Wkshp 4 - Workshop Goals

- Aligning Cultural values and digital security practices
- Guide organizational self-assessment of existing resources and practices
- Begin to articulate a stated security strategy/vision
- Hold discussions on policy building topics
- Dedicate time for individual security practices and 1:1 support
- Identify alignment or misalignment between values and practices, and work towards supporting practices that uphold our values
- Phase 1- Foundations: Ground Policies in the values of the organization & Build a Team
- Phase 2 – Build Collective Awareness: Knowledge Building & Political Education
- Phase 3 – Collaborative Policy Development & Develop an Incident Response Team

Stronger NYC Communities Organizational Digital Security Guide

Build Power - not Paranoia!

Visit: https://strongercommunities.info