Stronger NYC Communities Organizational Digital Security Guide

For Trainers and Participants

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.

INTRODUCTION

ORGANIZATIONAL DIGITAL SECURITY WORK IS IMPORTANT, RIGHT NOW.

Imagine you've just helped organize an immigrants' rights rally. You gathered thousands of names and email addresses from supporters of all kinds: first-generation immigrants, allies, undocumented people, clicktivist sideline watchers -- and everyone in between.

Looking at your list, things going through your mind might include:

- **How do I care for the information these people have shared with us?**
- **Can I help my coworkers care for this list?**
- **What about getting the list of their names and emails to a trusted partner?**
- **How do I make sure this list stays private?**
- **Should I even worry about this with everything else on my plate as an organizer?**

Now, imagine the winds have shifted in government practices -- you're growing more concerned about privacy and security, and you're organizing harder than ever. What do you do?

It's time to build your power, without letting worry and paranoia interfere with your strategic choices.

Read on to learn more about how you can:

- **Raise awareness around concepts in organizational digital security**
- **Give facilitators frameworks to facilitate hands-on practice with security tools and tactics**
- **Advance participant's organizational security practices via awareness, contextual understanding, strategies, and practice**
- **Build relationships of trust and a community of practice between trainers and participants**

Build Power - not Paranoia!

THE STORY OF THIS ORGANIZATIONAL DIGITAL SECURITY WORKSHOP GUIDE

Why we started this project

Vulnerable communities across New York City are seeing an increase in online and offline threats. These have ranged from cyber harassment, phishing and fraud/impersonation to questionable uses of their data.

The Stronger NYC Communities (SCNYC) project was designed to advance the digital security capacities of community-based organizations that work directly with immigrant populations. Importantly, these trainings address the unique challenges of participant groups as they tackle evolving digital security threats to their organizations, and to NYC residents whose data they collect, store and share.

Who the project designers are

This project was led by a team from Research Action Design (RAD) with funding from Mozilla Foundation, core partnership with Mayor's Office of Immigrant Affairs and the Office of the CTO of the Mayor's office of NY. A cohort of ten trainers who serve non-profit organizations stewarded the project together with RAD, facilitating five workshops over the course of six months with 16 community based organizations serving immigrant populations. We acknowledge also that this and all work draws on prior experience with individuals and organizations in the technology for social justice field and social movement.

This guide gathers all of this work - coordination, approach, train the trainer content, workshop facilitation guides, and a workbook for participants...

We hope you get a lot out of these!

HOW TO USE THIS GUIDE

This guide remixes and releases this work with the intention of allowing others to recreate this series. It includes instruction on our approach, facilitation and organization methods, full workshop facilitation guides, a workbook for participants, and a resource and training library.

This guide contains four main sections:

- **A guide to creating and facilitating organizational digital security workshops focused on supporting targeted communities**
- **A facilitator's manual, including workshop agendas, activities, handouts**
- **A participants handbook, including workshop outcomes, homework**
- **A resource guide and glossary.**

Read through the whole Guide, or pull out guidance, content, training activities, or agendas as-needed!

Themes

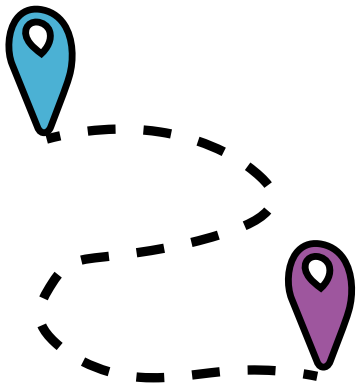
You will find in these guides activities for workshop settings to facilitate learning around:

- **Organizational Security Process:** From Risk assessment to policy writing
- **Tools and Tactics:** Hands on with tools and implementation strategies
- **Building Political Power:** Political history and collective approaches to increasing privacy and decreasing surveillance

ROADMAP

This guide will allow you to follow the organizational digital security workshop series we shared in NYC in 2017-2018, or mix-and-match to create your own workshops.

Whether you follow the workshop content we share closely, or create your own, here's your roadmap to doing this work.



Roadmap for Successful Organizational Digital Security Training

01 **Get a few people** to lead the digital security training project: facilitators and participant organizers. We recommend at least two facilitators per workshop, and more is ok!

02 **Prepare!** Read through the Prep, Design & Facilitation Guides, plan your workshop series timeline and start to book locations and trainers' meetings

03 **Participants!** Identify, invite, and pre-survey your **organizational participants**

04 Leader/facilitators **prepare for each workshop ahead of time** by assembling or using existing agendas, reading guides, print out handouts and activities etc.

05 **Host and lead the workshop(s)** making sure there's time for breaks and questions!

06 **Survey participants** to see how it went, what else they need, and how to improve - and debrief this information with the workshop leaders.

OUTCOMES FROM THIS WORK

Key outcomes from these workshops

1. Organizational Digital Security Process

Participants build capacity to steward digital security strategies in their organization. We share processes for building security into the culture of organizations and communities, beginning with risk assessments and following through to organizational policy creating and implementation. We address organizational change in a manner that sustains and honors the organization's own goals and processes, and respects the nature of this work as intensive, human-centered and emotionally charged.

2. Tactics and Tools: Hands-on and Implementation

Participants increase their practical skills with tools and implementation strategies. Topics range from document storage to device and account setup to change management in an organization.

3. 1-1 Support

Trainers accompany participants through the specifics of their organizational security processes. The training team directly supports the community-based organizations, offering online "office hour" skillshare sessions, and in-person support to facilitate the knowledge transfer and policy development by the community-based organizations.

4. Training of Facilitators

We build each other's capacities as facilitators through sharing knowledge and skill in organizational security and also through practical experience and development of facilitation skills.

5. Building a community of practice

Build relationships of trust and a community of practice between trainers and participants.

What's covered in the workshops

Workshop 1: Our work is political.

In Week 1, we introduce the principles of holistic security and the need for a holistic approach, and outline several goals we have for the coming weeks and months. We develop practices in all of these areas in the course of the following weeks.

Objectives:

- 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
- Develop risk assessment as a tool to bring back to each organization
- Understand why and how to use 2-factor authentication, strong passwords, and password managers to reduce unauthorized account access
- Recognize phishing attacks and identify ways to change phishing-vulnerable behavior

Topics we cover:

- State Surveillance, Colonialism, and Racism: a Brief History
- Risk Assessment: What it is, how to conduct risk assessments
- Holistic Security: What it is, why it's important
- 2-Factor Authentication
- Password Managers

The workshops are for adult learners who have many priorities, are part of organizations, and are connected to the reasons for doing digital security work.

Workshop 2: Our work is both individual and collective.

In Workshop 2, hear from guest speakers working in law and immigration justice. We take a step back and deepen your understanding of how the internet works, paving the way for a look at safer browsing habits and VPNs.

Objectives:

- Determine what data stewardship means to us as individuals and organizations
- Understand risks legal discovery poses to data privacy and security
- Deepen understanding of how networks and browsing work
- Gain familiarity with tactics and tools for network and browsing privacy and security
- Gain experience with VPNs
- Discuss motivation for increased browser privacy and security, and explore available tools

Topics we cover:

- Data stewardship and accountability
- Guest lectures: Speakers from NYCLU and Black Law Movement Law Project
- Understanding the internet: Networks, Wifi, Internet infrastructure and web requests
- Hands-on with VPNs

Workshop 3: Our work is about learning from and taking care of each other.

In Workshop 3, we shift focus to smaller group work, where we cover a range of hands-on topics from safer social media use to encrypted messaging. The majority of our work is in small groups, and we discuss organizational security and the elements for creating a security policy-making team in your organization.

Objectives:

- Support peer-sharing through facilitation and design of workshop
- 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

Topics we cover:

- Organizational security principles to enacting change
- Breakout Sessions: Hands-on topics reviews (Password Managers, 2-factor Authentication, VPNs and how to use them, Secure browsing)
- Breakout Sessions: New concepts (Encrypted video calling, Safer social media use, Action safety planning, Encrypted Messaging, Action Filming & Documenting safely)

Workshop 4: We do our best work when our values and practices align.

We tackle policy development topics and introduce concepts around policy and values alignment. The goal is to shift the conversation from the tools and tactics of the individual to the wider lens of how practices can become policies at an organizational level. We also revisit our breakout groups in order to have in-depth conversations on organization-level issues such as dealing with reluctance/disrupted workflows when adopting new security practices, tackling accusations of paranoia or frustration with new methodologies, and identifying realistic and achievable goals for your organization.

Objectives:

- Guide organizational self-assessment of existing resources and practices
- Identify team members who will support and drive policy drafting
- Begin to articulate a stated security strategy/vision and identify existing areas of alignment and improvement with this vision
- Create introduction to policy drafting plans to take back to organizations

Topics we cover:

- What alignment of values and practices looks like
- Self assessment: Where are our organizations in their policy-drafting process?
- Policy development working groups: fostering security culture, identifying goals, addressing the disruption of existing workflows, tackling paranoia, choosing alternative tools, and revisiting risk assessments
- Strengths Inventory/skillshare: Successful organizational tactics and campaigns

Workshop 5: Our work is ongoing. This is just the start of a longer, sustainable process.

In our final workshop, we combine some final skill-building sessions on encrypted file storage and backups with a team activity on incident response, which brings together everything we have worked towards in the previous four workshops.
We also debrief and wrap up as a group, looking at the ground we've covered, and get feedback on participants' experience.

Objectives:

- Learn about file and disk encryption
- Understand the importance of backups/redundancy and encrypted file storage
- Revisit safer social media use and how to choose and evaluate tools
- Synthesize concepts such as risk assessment, organizational policymaking elements, and concrete tools and tactics in team-based incident response scenario
- Debrief workshop series and collect exit metrics, feedback, and discuss goals for the project

Topics we cover:

- Encryption
- Choosing tools
- Safer Social Media II
- Backups and secure file storage
- Incident Response

So you're ready to start coordinating an organizational digital security workshop?

Start here!

In this section, we share best practices on:

1. Inviting and engaging Sponsors and Trainers
2. Suggested Collective Commitments
3. Creating a Safety Plan
4. Gathering and sorting Topics - including topic examples
5. Inviting Participants

Define the project

Decide who will lead the trainings

Perhaps it's you who's reading this, or perhaps you're hoping to engage other people. If you want to bring others in, it supports them to make their place in the project super clear.

1. Define the roles

Clear asks of everyone make it easier for people to say yes - they know what they're signing up for! For a multi-workshop project you might need lots of support.

Some roles you may want to define, like SCNYC did, include:

- Project Manager or Lead Coordinator
- Curriculum and Materials Lead Developer
- Documentation
- Facilitator or Facilitation Team

Optional: Invite more facilitators

2. Share the playbook

It's important for all stakeholders and participants - including trainer / facilitators and participants - to have a shared understanding of process: What the workshops are trying to do, why, and how.

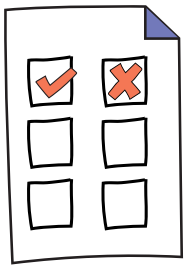
Sharing the playbook of agreements around how the workshops will operate and how we got to the topics being covered is a step - even better, use facilitation techniques (like we discussed in the last section) to invite dialogue and contributions to the topics and commitments to generate buy-in and group alignment on them.

3. Create a timeline, deadlines, and delegate tasks

Help everyone stay on the same page and move as a team - make sure folks' availability works for the plans and make clear asks.

For example, we mapped out all the workshops and preparation meetings at the beginning of the series, about two months before starting, so that everyone was able to find and secure their availability.

Collective Commitments, Workshop Agreements & Values



Collective Commitments, Workshop Agreements & Values should be co-created at the beginning of the series with the leadership and trainer/facilitators. Once you have participants -- bring them into the process and ask if they have more Agreements to contribute. Finally, returned to these at the beginning of each workshop if you're making this a series.

These are ones used in the Stronger Communities project. Feel free to use them as well as a starting point, or completely design and customize your own.

Everyone is an expert

- The implementing team, trainers, participants, and 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.

Any question is a good question (but get to the point)
"One Mic" - don't interrupt
Harm reduction

- The practices taught should reduce, not provoke anxiety, and should allow for a series of incremental improvements that fit with organizations' needs.
- Organizations will be met where they are at without judgment or evaluation, and will not be given a 'security prescription.'

Consent-based sharing practice

- Make sure that private details stay private, while important information travels out
- Often expressed as: "what's learned here leaves here, but what's said here stays here"

Don't use jargon and spell out acronyms

- Design holistic and sustainable strategies
- 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.

Build Power, not Paranoia!

Be 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.

Creating a Safety Plan

You need to be aware that gathering a group of people who care about and/or who may be immigrants creates the possibility of being targeted for surveillance - or other nefarious activity.

Knowing this, it is in your and all your participants' best interest to create a safety plan.

This can include:

1. **Getting emergency contacts for everyone participating, and sharing under what circumstances they would be used**

2. **Defining an Incident Response Plan. Here's the one we used:**

- In case of any safety or security incident, [project coordinators] will send communication via the [trainers email list]. They will first get consent of any people involved in the event before sharing.
- If an incident relates to just a single person, they will work with that person's emergency contact to support the person.
- If the incident impacts more than one person, the workshops themselves, etc, [project coordinators] will escalate to inform project sponsors.

3. **Getting and sharing Workshop Site Safety Information, like:**

- Point of Contact for the training site: Name, Mobile, Email, Relationship to program
- Safety route out of the building/Safety plan for building
- Policy of who you will and won't let in [in particular, look for a policy disallowing different government agencies to enter without a warrant]
- What are our rights in that building?

4. **Inviting participants to activate their own safety networks, for example sending them an email like this one:**

Dear Participants,
As part of our safety planning for the workshops, please share information with a manger or a colleague at work about your participation in Weds' training. If participating in this workshop is sensitive for you, please also set up a relevant check in system with your point of contact – ex. Check in when you arrive at the workshop, check in when you leave, check in when you get to your next destination.

5. **Identifying Legal support networks available to you**

6. **Sharing with everyone involved that there is a Safety Plan**

Workshop Topics

In the last chapter we gave you a snapshot of the workshops this Guide covers.

Here's a pared-down list you can use when planning your workshop and preparing to ask participants what they might want to learn.

Organizational digital security topics we covered, and which participants asked for are:

- **Encrypted Messaging (Signal, WhatsApp)**
- **Full Disk Encryption on computers**
- **2-Step Verification / 2-Factor Authentication**
- **Organizational Security Policies**
- **Security Workshops and Trainings**
- **Risk Assessments**
- **Password Managers**
- **Encrypted Email**
- **Encrypted Documents**
- **Encryption Tools**
- **Privacy-friendly browser extensions such as HTTPS Everywhere, Privacy Badger**
- **Regular Software and Operating System Updates**
- **Regular Data Backups**
- **VPN**

And of course - Invite Participants and see where they are at!

Identify & Invite Participants

Community groups you're part of, organizations you have connections to, and/or social groups you interact with are all great places to find participants.

For the SCNYC project, we invited organizations to send two participant representatives per organization, so as to generate internal support for the participants and distribute learning using a train-the-trainer model. This also allowed us to scale our impact, as we focused on organizations that had community reach and were valued leaders in their work.

If you're not directly connected with community groups, note that given the nature of digital security focused on supporting targeted communities such as immigrant groups, you will certainly want to partner with trusted persons and/or organizations.

Assess Participant needs

See a sample Organization Needs Assessment Worksheet in the next chapter: ***Evaluation.***

Once you've identified and invited participants and gotten a yes, you may want to survey them to assess where they are currently with their digital security concerns, practices, and needs to understand how you might best serve them and compare their knowledge before and after for evaluation.

Facilitation & Workshop Design Techniques

A workshop is an intentional space, created for learning, changing points of view, and people leave with clear actions to take. Part of the power of a workshop is in its design and its leadership.

In this section, you'll learn:

- **Facilitation Practices: General and Advanced Pro-tips**
- **An intro to Open Space sessions - and how to run them**
- **How to hold space for the Emotional Aspects of the Work**

General Facilitator Practices

This is a quick list that trainer/facilitators might want to read and remind themselves with before any workshop session.

Checking in
Use a few minutes at the beginning of the workshop and after beaks to bring everyone together (for example, with an icebreaker). This allows facilitators to both understand the energies that people are arriving with and request that participants focus their attention on the workshop.

Participants in the lead
Whenever possible, ask participants if they want to share their knowledge and experience rather than explaining something yourself. The workshop has to have meaning to our participants and be driven by their needs and experiences, so the more they drive it, the better.

Open Space
Open-space sessions are a format for holding self-organized sessions around a certain topic or theme. In general they are open-ended and emphasize the knowledge, emergent creativity, and resources of the participants who are present, rather than a predetermined idea of what should be discussed and decided.

Keeping energy up
Bring snacks and beverages and encourage a room setup where it's easy to get up, stretch your legs, and grab a drink or a bite during the session.

Co-facilitate
Agree with your co-facilitator(s) on methods to communicate around the energy and needs in the room including:

- **Responding to questions in the room.** For example, as a co-facilitator you could raise your hand and ask guiding questions of the lead facilitators when you know participants have questions.
- **Maintaining a calm pace and slowing down.**
- **Taking a break or doing an ice-breaker.**
- **Keeping time.**

Be prepared
Prepare yourself and with your co-facilitator(s) to facilitate a clear space for learning and building. Read through the handouts and facilitation guide ahead of time. Prepare your facilitation with your co-facilitator(s), knowing what roles you will take in the workshop.

Prepare for the Emotional aspects of security work
Especially, avoid paralysis (a/k/a 'security nihilism') by making sure to identify strengths at the same time as identifying challenges/risks.

Open Space

In your workshops, we suggest employing the principles of open space meetings while addressing specific topics in digital security.

Running an Open-Space-Like Session

A lot of the work we did was focused on small group conversations.

If you want to run these types of sessions, here is a guide to help you get started.

Background: Open-space sessions are a format for holding self-organized sessions around a certain topic or theme. In general they are open-ended and emphasize the knowledge and emergent creativity of (and resources) of the participants that are present, rather than a predetermined idea of what should be discussed and decided.

Setup:

- Chairs in a circle so that we can all see each other and reduce hierarchy of seating placement.
- Writing/documenting materials available (paper, markers, whiteboard, handouts, etc).

The principles of open-space workshops:

- "Whoever comes is the right people.
- Whenever it starts is the right time.
- Wherever it is, is the right place.
- Whatever happens is the only thing that could have happened. Prepare to be surprised!
- When it's over, it's over."

And finally, "If you're in a situation where you're not contributing or learning, you're free to move to a different space." Your participants should feel free to stay in the space as long as it is serving them, and should feel safe moving to a different space (non-disruptively!) if they so choose.

Further reading on Open Space design:

http://www.michaelherman.com/cgi/wiki.cgi?OpenSpaceTechnology
http://www.openspaceworld.com/users_guide.htm
https://en.wikipedia.org/wiki/Open_Space_Technology
http://www.communityplanning.net/methods/open_space_workshop.php
http://www.openspaceworld.org/files/tmnfiles/OSTResearch2000.htm

Prepare for the Emotional aspects of security work

Creating the organizational climate that's open to security work means being in alignment with these principles, and maybe others that you hold as well.

- **Manageable, incremental improvements.** People won't adopt to a shock to the system in terms of a barrage of new tools, procedures, or devices; they will feel stressed, frustrated, and disempowered. People are also creative; frustration around new tools or procedures is a natural breeding ground for 'shadow architecture' (i.e., more convenient but less secure workarounds that people adopt when they're frustrated or overwhelmed). It can be hard to balance the urgency and importance of the information you're conveying with the rate at which folks can absorb it, but proceed slowly and check in as you go.

- **A culture of welcoming all questions.** Both in the training space and in each organization's space, there needs to be a safe and well-communicated culture for bringing up questions. If everyone else seems to be following a high-level conversation, it can be difficult or intimidating to ask a question like 'what is encryption?', or it can seem disloyal or skeptical to ask 'why do we even need to do this at all?', but both types of questions need to be welcomed - both to make sure everyone understands and can follow any new organizational practices, and because sometimes, dissenting or reframing questions can actually prompt the most important realizations and tactics.

- **Appropriate pacing.** Some topics will spark more of a discussion with some groups than others. Trust this and use your judgment in reworking the sessions.

- **Avoiding paralysis**/'security nihilism' by making sure to identify strengths at the same time as identifying challenges/risks. We will continually revisit the stories of both internal and collective resilience (which is why we're doing this work in the first place!). Our strongest tactics remind us of our existing strengths.

- **Checking in as we go.** it's more important to cover material well than it is to push through all of it. If people are stressed or overloaded, they won't learn. Pay attention to the energy in the room and change plans if necessary.

Facilitation and Design approaches

These workshops are for adult learners who have many priorities, are part of organizations, and are connected to the reasons for doing digital security work.

Methods we wove into the design and facilitation of the workshops included:

- Participatory design - getting all engaged and involved
- Pop education - drawing from people's existing knowledge
- Intersectionality - acknowledging that people are complex and bring multiple identities and experiences into the room

A few facilitation resources

ADIDS: Adult learning methodology by LevelUP: Activity & Discussion, Input, Deepening, and Synthesis
https://www.level-up.cc/before-an-event/preparing-sessions-using-adids/

Anti-Oppression Resource and Training Alliance (AORTA)
http://aorta.coop/portfolio_page/anti-oppressive-facilitation/

Facilitating Group Learning: Strategies for Success with Adult Learners, by George Lakey

Popular Education
http://www.practicingfreedom.org/offerings/popular-education/

Training for Change
https://www.trainingforchange.org

EVALUATION

EVALUATION

Often, evaluation is a key way we're able to generate trust in - not to mention funding for! - our work as trainers. Don't overlook it. Instead, use evaluation as a way to make sure your workshops are as useful as possible for your participants.

Setting a rhythm of surveys

Setting a cadence of regular, brief surveying helps your participants expect to be surveyed, and can increase return rate. It also helps you as a workshop leader remember to survey and evaluate -- and gives you data you can use to measure outcomes (something our sponsors and funders tend to like) and improve future workshops.

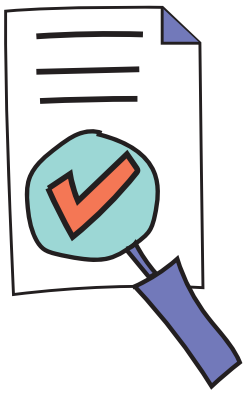
If you delivered a pre-Workshop assessment when you invited your participants (see the previous section), you are already off to a good start.

Delivery notes for facilitators

- **Evaluate early and often!** It gets people used to it, and gives you lots of ideas and participant-focused guidance to learn and improve from.
- **A written evaluation** works best if you hand it out before the end of a workshop session and build in about 10 minutes for people to fill it out before they have to leave. Also, shorter surveys get longer answers to the particular questions.
- **A verbal evaluation** is great for asking deeper questions, and can be connected to an ongoing 1:1 meeting or administered in a pre-scheduled time.

You can print the following pages

SAMPLE EVALUATIONS



Below are four evaluations. Here's when and how you'd use them.

1. Intake Assessment - To intake organizations or participants into a workshop or workshop series. Feel free to customize the following intake assessment, which is keyed to organizations who are sending one or more participants to the workshop. You might use it for a verbal intake over the phone or on a video call, or send it as an email or as a document you have someone fill out and return, as it's a bit long for a form.

2. Training Evaluation: Written - use this as a handout at the end of the first or second workshop to touch base with participants and see what they're getting out of the workshop.

3. Mid-Series Evaluation - Can be a verbal check-in or a handout. Use this after the second or third in a series of workshops to see if the participants are getting what they need, and to guide changes to your content or approach if needed.

4. Exit Survey - a full check-out survey, designed to be sent as a form or given as a handout to dive deep into outcomes and transformations the participants experienced from a series of workshops.

1. Intake: Organization Representative Assessment Worksheet

Purpose of this assessment

- Develop a program that is grounded in the goals of participating organizations
- Develop understanding of participating organization and how it will implement change
- Gather participating organization's goals
- Assess any major areas of concern

Organization Blurb / Mission+Vision:

Current Main areas of work:

Organizational Structure: What is the organizational structure? Who manages IT? What do they manage (ex. Servers, email, wifi?

Organizational Change: How will you bring the processes and learning from this project into your organization? Who else will you work with to make decisions and implement?

Organization Goals: What are your organization's goals for participating in this program?

This assessment template developed by RAD for this SCNYC includes best practices learned from Association for Progressive Communications (APC), Security Positive, and Wellstone.

Current Practice: How does your organization address safety concerns?

Greatest Concerns: What are your greatest concerns regarding your organization's members, staff, supporters' safety?

Risk Assessment Storytelling

- What security issues have you or members of the organization already experienced?
- What happened? Where? How? What was the threat?
- What was the impact of that incident/threat: to self, the community, the work?
- What did you do in response to the threat? How did others help?

Mapping Questions

- What kinds of data do you work with?
- Data gathered on members? Grantees? Partners?
- What is the most sensitive data you work with? And how do you take care of it?
- What software and tools do you work with (ex. Google Suite, Office 365, Dropbox)?
- What are your backup processes?
- Do you have any concerns about how you gather or manage data?
- What software and tools do you use to communicate with staff / volunteers / clients / members?
- What software tools do you use to communicate with staff / volunteers / clients / members?
- What is the most sensitive communication you do? And how do you take care of it?
- What kinds of devices do people use for work (ex. desktops, laptops, mobiles)? What security protocols do you have in place for these?
- How do you secure your offices (ex. Doors, cabinets, offices)?
- Do you have any specific concerns about your offices?

2. Training Evaluation

- During this workshop, what worked for you? Please be specific, with examples:

- What didn't? Please be specific, with examples:

- What key takeaways did you get out of the workshop?

- What do you need more of to support you applying strategies, tactics, and tools from the workshop in your organization?

3. Mid-Series Workshop Evaluation

- Since your first workshop, what practices or tools did you implement?

- What else do you need support with?

- Is there anything you want to contribute?

- What are your goals for the rest of the training? Have they changed?

4. End of Workshop Series Exit Survey

Please select the topics, if any, you were familiar with, ***BEFORE*** the Stronger Communities Workshop began.

- 2-Step Verification / 2-Factor Authentication
- Encrypted Documents
  Encrypted Email
- Encrypted Messaging (Signal, WhatsApp)
- Encryption Tools
- Full Disk Encryption on computers
- Organizational Security Policies
- Password Managers
- Privacy-friendly browser extensions such as HTTPS Everywhere, Privacy Badger
- Regular Data Backups
- Regular Software and Operating System Updates
- Risk Assessments
- Security Workshops and Trainings
- VPN

Please select the topics, if any, you are familiar with now, ***AFTER*** the Stronger Communities Project.

- 2-Step Verification / 2-Factor Authentication
- Encrypted Documents
- Encrypted Email
- Encrypted Messaging (Signal, WhatsApp)
- Encryption Tools
- Full Disk Encryption on computers
- Organizational Security Policies
- Password Managers
- Privacy-friendly browser extensions such as HTTPS Everywhere, Privacy Badger
- Regular Data Backups
- Regular Software and Operating System Updates
- Risk Assessments
- Security Workshops and Trainings
- VPN

What is the most important thing you feel you have learned in the Stronger Communities project?

Which of the following were the ***MOST*** helpful, interesting, or positive parts of the Stronger Communities project? (You may select more than one)

- Whole group discussions
- Lecture/Instruction
- Demos
- Online office hours/clinics
- Guest speakers
- 1:1 Support in person
- Phone checkins
- Small group (2-3 person) discussions
- Other:

Which of the following were the *LEAST* helpful, interesting, or positive parts? (You may select more than one)

- Small group (2-3 person) discussions
- Guest speakers
- Lecture/instruction
- 1:1 Support in person
- Demos
- Whole group discussions
- Online office hours/clinics
- Phone checkins
- Other:

If you selected items on the last question, can you please elaborate on why those things were not helpful, interesting, or positive?

Do you have any comments or suggestions on things that would have made our workshops more helpful to you?

My organization talks about digital security practices with employees (in staff meetings, trainings, etc).

Not very true Very true
1 2 3 4 5

My colleagues are open to changing their digital practices.

Not very true Very true
1 2 3 4 5

My supervisors / managers are open to changing their or digital practices.

Not very true Very true
1 2 3 4 5

My organization has a full-time IT person.

Yes
No

This is the area I feel my organization does **BEST** at with regards to organizational or digital security:

This is what my organization most urgently needs in order to strengthen its digital security:

After completing this program, are you now more or less confident about how your organization handles its data?

- Much more confident
- Somewhat more confident
- No change in confidence
- Somewhat less confident
- Much less confident

Activity & Handout Glossary

A quick reference for facilitators to pick out handouts or activities to use in workshops.

Handout List

Handout name	Used in workshop	Participants find it...
Risk Assessment Walkthrough	1: Principles & basics of holistic security	Facilitators print and bring as prep for workshop 1, it's attached to the Facilitator Guide
NYCLU NY ECPA Fact Sheet (2017).pdf	2: Data Security	Attached to the Participant Workshop Guide. Facilitators also have a prompt to print it for participants.
Ways to Protect Your Cell Phone (2017).pdf	2: Data Security	Attached to the Participant Workshop Guide. Facilitators also have a prompt to print it for participants.
Practices in Organizational Holistic Security - Preparedness Assessment	3: Organizational Digital Security	It's in the Participant Guide for Workshop 3
Handout: Organizational Security: Towards a Policy Development Process	3: Organizational Digital Security	Facilitators print and bring as prep for workshop 3
Aligning Values and Practices Adapted from Cultural and Digital Security Practices by Kyla Massey	4: Policy & Procedure	In Workshop 4 Facilitators' Guide and Participant Workshop Guide.
Addressing Proficiency Gap	4: Policy & Procedure	In Workshop 4 Facilitators' Guide and Participant Workshop Guide.
Alternatives to Google Docs	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Are you just being Paranoid? One Sheet	4: Policy & Procedure	In Workshop 4 Facilitators' Guide

Handout name	Used in workshop	Participants find it...
Intergenerational Working Group Handout	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Creating Prioritized Goals Worksheet	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Open Space Mini-Workshop Tool Handouts	5: Incident Response & Wrap up	In Readings & Resources
Incident Response Scenario	5: Incident Response & Wrap up	In Workshop 5 Facilitators' Guide

Activity Glossary

Activity name	Used in workshop...	Facilitators find this...
History of Surveillance	1: Principles & basics of holistic security	In Workshop Facilitators' Guide for Workshop 2
Holistic Security Process: Risk Assessment	1: Principles & basics of holistic security	In Workshop Facilitators' Guide for Workshop 2
What we know: Mapping exercise	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Data My Organization Collects	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Internet Structure (Matching Cards)	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Browsing / Browsers	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
VPN Demo	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Putting it Together: Organizational Security Process	3: Organizational Digital Security	In Workshop Facilitators' Guide for Workshop 3
Open Space Mini-workshop	3: Organizational Digital Security	In Workshop Facilitators' Guide for

Activity name	Used in workshop...	Facilitators find this...
Facilitator Guides	4: Policy & Procedure 5: Incident Response	Workshop 3, 4, 5
Open Space Mini-workshop Support Materials	3: Organizational Digital Security 4: Policy & Procedure 5: Incident Response	In Readings & Resources, section *"Open Space Tool Handouts"*
Drafting Organizational Policy: Breakout Session Topics	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Aligning Values and Practices	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Incident Response Scenario	5: Incident Response	In Workshop 5 Facilitators' Guide (with handouts in the Guide)
Group Timeline	5: Incident Response	In Workshop 5 Facilitators' Guide (with cheat sheet in the Guide)

STRONGER NYC COMMUNITIES
FACILITATOR GUIDE

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

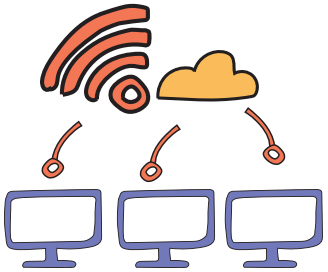
Print the following data security guides:

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.

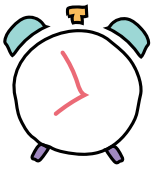
Framework: Your homework was to do:

- 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

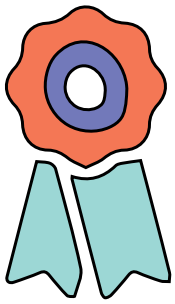
Discussion: What do we know about VPNs?

- 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

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.

Open space session:

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

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

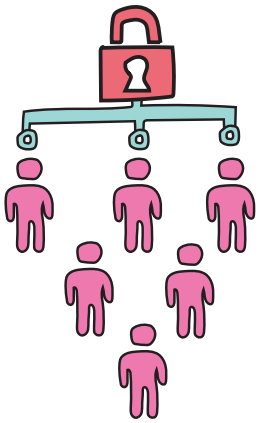
Anonymity & Privacy discussion

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
FACILITATOR GUIDE

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

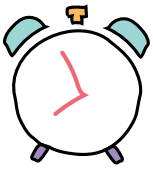
Room set up needs:	Materials to print and prepare	Activities
Name tags, markers, Post its	Agreements / Community Guidelines	Review Mind mapping homework from Workshop 3
Snacks and coffee/tea? (Make a plan if you want these)	Homework / Workshop handout	Group Discussion: Aligning Cultural and Digital Practices
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		

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.

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.

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."

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"

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

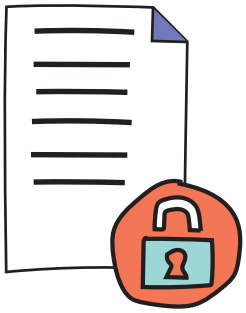
- Aligning Cultural values and digital security practices
- Guide organizational self-assessment of existing resources and practices
- Begin to articulate a stated security strategy/vision
- Hold discussions on policy building topics
- Dedicate time for individual security practices and 1:1 support
- 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

Participant Workbook

How to Build Power - not Paranoia in your Organization!

What's covered in the workshops



Workshop 1: Our work is political.

In Week 1, we introduce the principles of holistic security and the need for a holistic approach, and outline several goals we have for the coming weeks and months. We develop practices in all of these areas in the course of the following weeks.

Objectives:

- 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
- Develop risk assessment as a tool to bring back to each organization
- Understand why and how to use 2-factor authentication, strong passwords, and password managers to reduce unauthorized account access
- Recognize phishing attacks and identify ways to change phishing-vulnerable behavior

Topics we cover:

- State Surveillance, Colonialism, and Racism: a Brief History
- Risk Assessment: What it is, how to conduct risk assessments
- Holistic Security: What it is, why it's important
- 2-Factor Authentication
- Password Managers

Workshop 2: Our work is both individual and collective.

In Workshop 2, hear from guest speakers working in law and immigration justice. We take a step back and deepen your understanding of how the internet works, paving the way for a look at safer browsing habits and VPNs.

Objectives:

- Determine what data stewardship means to us as individuals and organizations
- Understand risks legal discovery poses to data privacy and security
- Deepen understanding of how networks and browsing work
- Gain familiarity with tactics and tools for network and browsing privacy and security
- Gain experience with VPNs
- Discuss motivation for increased browser privacy and security, and explore available tools

Topics we cover:

- Data stewardship and accountability
- Guest lectures: Speakers from NYCLU and Black Law Movement Law Project
- Understanding the internet: Networks, Wifi, Internet infrastructure and web requests
- Hands-on with VPNs

Workshop 3: Our work is about learning from and taking care of each other.

In Workshop 3, we shift focus to smaller group work, where we cover a range of hands-on topics from safer social media use to encrypted messaging. The majority of our work is in small groups, and we discuss organizational security and the elements for creating a security policy-making team in your organization.

Objectives:

- Support peer-sharing through facilitation and design of workshop
- 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

Topics we cover:

- Organizational security principles to enacting change
- Breakout Sessions: Hands-on topics reviews (Password Managers, 2-factor Authentication, VPNs and how to use them, Secure browsing)
- Breakout Sessions: New concepts (Encrypted video calling, Safer social media use, Action safety planning, Encrypted Messaging, Action Filming & Documenting safely)

Prepare to start!

Expect to share
The trainers and facilitators will ask for your input, on intake, in the workshops and afterwards.

Be ready for the emotional aspects of security work
Creating the organizational climate that's open to security work means being in alignment with these principles, and maybe others that you hold as well.

Your trainers will commit to the following, and we ask you to do the same:

- Manageable, incremental improvements.
- A culture of welcoming all questions.
- Appropriate pacing.
- Avoiding paralysis
- Checking in as we go

Know what Open-Space sessions are
Here is information on the way we run our breakout sessions. **Open-space sessions** are a format for holding self-organized sessions around a certain topic or theme.

In general they are open-ended and emphasize the knowledge and emergent creativity of (and resources) of the participants that are present, rather than a preordained idea of what should be discussed and decided before the workshop. Participants drive the content, and facilitators and other participants provide the information.

If you want to run these types of sessions at your own organization, see the facilitator's guide for more information on how to run Open Space.

After the workshops

Whether you read this online, take one workshop, or attend all five workshops in the full series, the next steps are ones you have to take, ideally with the full collaboration and support of the folks in your organization

Digital Security at the organization level is a process that you build with other people. It's another way of being in relationship with respect and care

We hope you get a lot out of these workshops and resources - you can find more to support you in the resources, and linked at: https://strongercommunities.info

Play a Digital Hygiene game to get ready!

Digital hygeine bingo I: examples of personal strategies/practices

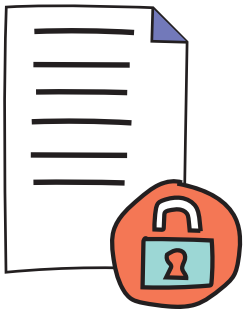
Do these practices apply to you? Do other practices apply to you?

I don't reuse any passwords.	I use Privacy Badger, UBlock Origin, and HTTPS Everywhere*, or comparable tools, to limit my browser fingerprint.	I have data backups; if my laptop or phone fell in the ocean tomorrow, my passwords and files would not be gone forever.	I use a VPN (and I know why I/we chose that VPN provider!)	I don't* click on links from URL shorteners
I don't download extra apps or games on my work devices; I have as few programs as possible.	Macros are disabled on my MS Office suite	My phone receives timely operating system updates and security patches.	I install operating system and system software updates on my laptop.	Files on my laptop are encrypted, or my whole laptop is encrypted.
I use 2-factor authentication as many places as possible (and have saved my backup codes somewhere safe!).	My security questions could not be answered by someone who looked up publicly available information about me.	**Free <3**	I use a password manager for most or all of my passwords*.	My phone is encrypted and my SIM card is encrypted (I need to enter 2 PINs/ passwords when I turn my phone on)
I have a or no clicking* (or careful clicking) policy for links in emails.	I install operating system updates on my phone.	I use Signal or WhatsApp (end-to-end-encrypted text messaging platform) instead of* plain text messaging.	I verify 'off-band' with people if I receive any communication (email, text) from them I'm unsure about.	I know how to use Tor browser to do sensitive research.
I don't leave my laptop unlocked or unattended.	I use appear.in, jitsi, or another encrypted video chat platform, instead of Skype	I Google myself or have a friend Google me periodically (with a VPN on or via Tor) to see what information is publicly available.	I use private browsing and know how to delete/clear cookies.	My social media and online accounts have restricted privacy settings and show limited revealing information about me.

Workshop 1
PARTICIPANT WORKBOOK

Workshop 1: Our work is political.

What you'll learn in this workshop:



- An 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
- 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)

Reading:

- See the first section in the Resources chapter to learn more about surveillance tactics over time.
- Read the Phishing section in the Resources chapter.

Homework & Next steps:

Activities: The following build on our workshop. Please get started on these, and bring updates on how it's going to the next workshop.

1. Risk Assessment - Preparation Work

- Facilitate a risk assessment conversation with your organization.
- Ground this conversation in the values and vision of your organization.

Bring back at least two examples of risk scenarios your organization discusses to Workshop 2.

Suggested prompts for grounding in values and vision:
- 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?

A risk assessment answers the following questions:

- What do we have that we may want to protect? (Pick something specific).
- Who or what might we want to protect it from? How likely are they to succeed?
- What are the consequences if they do succeed? Who is most impacted?
- What steps are we currently taking to reduce this risk?
- What else can we do?

2. Protecting Passwords - Preparation Work

This activity involves using a password manager, setting up 2-factor authentication (2fa), and mapping out if your organization uses shared accounts.

- **Start by choosing a password manager.** Pick a long, strong master passphrase and don't lose it! This could be your most important password!

- **Identify some accounts** that you use and store your passwords in your password manager. Practice using your password manager to log in and out of accounts.

- **Setting up 2-factor authentication (2FA):** pick a service you use that supports 2fa (such as Gmail, Facebook, etc). Start with an account that only you access. Download a 2-factor app (Google Authenticator or Authy) and enable 2-factor authentication for this account. Store your backup codes somewhere safe (for example, in your password manager).

- **Shared Accounts:** It's possible to set up 2fa on shared accounts, but it's a good idea to examine whether it's strictly necessary to share this account. If accounts are shared at your organization, write down what kind they are (social media, email, etc.) and who has access, and why the accounts are shared.

3. Tools, tactics, practices: a checklist

How likely are you to adopt the following tools and tactics? Which ones would create pushback or be difficult to adopt in your organization and why?

You can write a checkmark, X, or ? question mark beside each tool or tactic.

Password strength

- Choosing secure passphrases
- Setting up 2FA and saving backup codes
- Using unique passwords
- Using a password manager

Organizational

- Reviewing risk assessments periodically
- Talking to colleagues about risks they perceive

Fostering a digital communication culture (email/text, etc) that makes phishing behaviour stand out

- Avoiding URL shorteners
- Verifying 'off-band' if an email or text seems suspicious
- "Careful Clicking": Typing links in your address bar instead of clicking through from emails
- Careful downloading or no/low attachments policy: double checking before downloading attachments, opening attachments in another environment (Google Drive, Virustotal, virtual machine) first/instead

Workshop 2
PARTICIPANT WORKBOOK

Workshop 2: Our work is both individual and collective.

What you'll learn in this workshop:

- Determine what data stewardship means to us as individuals and organizations
- Know how data moves on the internet and why it matters
- Gain understanding of data confidentiality and practices
- Deepen understanding of how networks and browsing work
- Know what's a VPN is and gain hands-on experience with VPNs and
- Gain familiarity and motivation for increased browser privacy and security, and explore available tactics and tools

Homework and Practice

- See the first section in the Resources chapter to learn more about surveillance tactics over time.
- Read the Phishing section in the Resources chapter.

Homework & Next steps:

Congratulations! You are are on your way towards connecting principles with practices--what drives your work, what tools you're already using to further goals, and other options to explore.

1. Building Political Power: Data Practices

Facilitate a conversation around data practices for your organization.
- What are your data collection policies now?
- What types of data do you steward?
- Is there scope for applying lean (less) data collection policies or shifting your existing practices?

2. Hands on: Choosing a VPN

- Based on our conversations and what criteria is important to you, choose a VPN that works for you, and try using it.
- You can refer to https://thatoneprivacysite.net/simple-vpn-comparison-chart/ (in depth!), research using the Resources on the next pages, or ask facilitators if you are looking for additional resources.
- Some paid VPNs have free demo versions that you can use to see which ones you like.
- You can use https://www.dnsleaktest.com/ to check if your IP address is being leaked or not once you have your VPN set up.

3. BONUS: Holistic Security: Access Mapping, Organizational Policies.

Imagine a staff person who is new to your organization. What would their "onboarding" process--that is, the time that they are brought into the company and getting set up as a new employee/volunteer--include? At what point would they gain access to credentials such as: an email address from an organization's domain, (newstaff@myorganization[.]com), a shared organizational account (email or social media), office keys, personnel files, or other data or resources that you steward?

Conversely, when a staff member leaves, is there a checklist that is gone through to make sure that they don't have any lingering access to services or resources that they shouldn't (such as accounts or passwords, billing/banking information, or even wifi credentials)? Is that process different if someone quits or is fired?

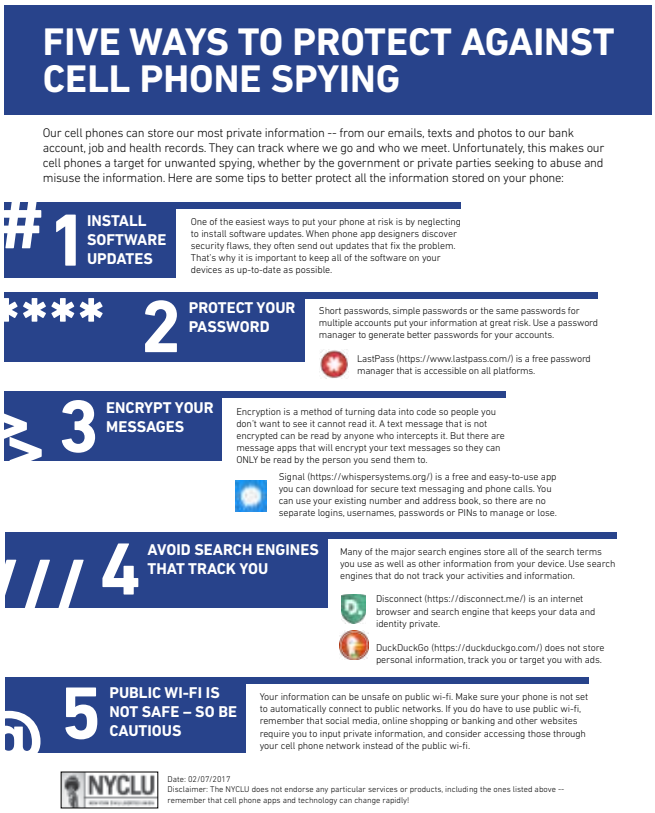
Begin to draft a checklist of 'services this employee can access,' and how soon they can access them (1 week, 3 months, immediately, never without supervision, etc).

Also begin to draft a checklist of what happens when this employee/ volunteer's time working with you comes to an end--are their accounts deactivated? are passwords changed? are office credentials changed? etc.

We will use these two checklists next workshop to begin examining organizational policies.

IMAGES FOR VISUAL REFERENCE ONLY:

1. https://drive.google.com/file/d/1aKs83UL-vScLMOCwjk-t4KWwwbedmKeT/view
2. https://drive.google.com/file/d/1qze3i8E1eIp8TSRy3LyDYaKqKX_WZsgE/view



FIVE WAYS TO PROTECT AGAINST CELL PHONE SPYING

Our cell phones can store our most private information -- from our emails, texts and photos to our bank account, job and health records. They can track where we go and who we meet. Unfortunately, this makes our cell phones a target for unwanted spying, whether by the government or private parties seeking to abuse and misuse the information. Here are some tips to better protect all the information stored on your phone:

#1 INSTALL SOFTWARE UPDATES

One of the easiest ways to put your phone at risk is by neglecting to install software updates. When phone app designers discover security flaws, they often send out updates that fix the problem. That's why it is important to keep all of the software on your devices as up-to-date as possible.

****** 2 PROTECT YOUR PASSWORD**

Short passwords, simple passwords or the same passwords for multiple accounts put your information at great risk. Use a password manager to generate better passwords for your accounts.

LastPass (https://www.lastpass.com/) is a free password manager that is accessible on all platforms.

3 ENCRYPT YOUR MESSAGES

Encryption is a method of turning data into code so people you don't want to see it cannot read it. A text message that is not encrypted can be read by anyone who intercepts it. But there are message apps that will encrypt your text messages so they can ONLY be read by the person you send them to.

Signal (https://whispersystems.org/) is a free and easy-to-use app you can download for secure text messaging and phone calls. You can use your existing number and address book, so there are no separate logins, usernames, passwords or PINs to manage or lose.

4 AVOID SEARCH ENGINES THAT TRACK YOU

Many of the major search engines store all of the search terms you use as well as other information from your device. Use search engines that do not track your activities and information.

Disconnect (https://disconnect.me/) is an internet browser and search engine that keeps your data and identity private.

DuckDuckGo (https://duckduckgo.com/) does not store personal information, track you or target you with ads.

5 PUBLIC WI-FI IS NOT SAFE – SO BE CAUTIOUS

Your information can be unsafe on public wi-fi. Make sure your phone is not set to automatically connect to public networks. If you do have to use public wi-fi, remember that social media, online shopping or banking and other websites require you to input private information, and consider accessing those through your cell phone network instead of the public wi-fi.

NYCLU

Date: 02/07/2017
Disclaimer: The NYCLU does not endorse any particular services or products, including the ones listed above -- remember that cell phone apps and technology can change rapidly!

The New York State Electronic Communications Privacy Act (NY-ECPA, A. 1895)

Summary

The New York State Electronic Communications Privacy Act safeguards the electronic information of New York residents and supports innovation by updating state privacy law to match our expanding use of digital information.

Existing privacy laws require the police to get a warrant before searching the file cabinet or computer in your house or the letters in your mailbox. Now that technology has advanced, New York state laws need to be updated to require the same warrant protections when the police want to track your phone or read your emails, text messages, online records or social media.

Background

New Yorkers increasingly rely on cell phones, computers, tablets and the internet to connect, communicate, work, research information and manage often sensitive or confidential personal matters. Low-income New Yorkers and New Yorkers of color are particularly dependant on their cell phones for online access.[1]

Our privacy laws must advance at the same pace as technology because law enforcement is increasingly taking advantage of new technologies to access our information. For example:

- In the first half of 2015, Verizon received 149,810 law enforcement requests for customer data, **only 10 percent** with a warrant.[2]
- In 2015, Twitter received more demands from New York law enforcement than **any other state**.[3]
- New York law enforcement sent more requests to Tumblr in the **first half of 2015** than it did in all of 2014.[4]
- The number of user information requests to Snapchat **almost doubled** in the first half of 2015, even though most Snapchat users believe their photos, videos and texts get deleted.[5]
- In the first half of 2015, Facebook received **17,577 requests** from federal, state and local law enforcement regarding **26,579 accounts**. Information was produced in 79.8 percent of cases.[6]

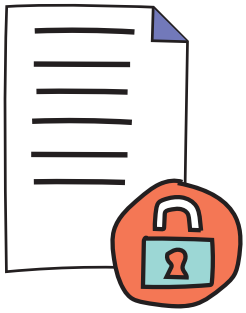
As a result, public confidence in technology is decreasing, and companies are concerned about developing new technology. According to the Pew Research Center:[7]

- 80 percent of adults feel that Americans are rightly concerned about government monitoring of internet communications.
- 70 percent of social networking users express concern about government access.
- 75 percent believe that their email messages, texts and location are sensitive.

Courts and legislatures around the country are recognizing the need to update privacy laws for the digital age, and the White House has also called on lawmakers to update the law.

Workshop 3
PARTICIPANT WORKBOOK

Workshop 3: Our work is about learning from and taking care of each other.



What you'll learn in this workshop:

- How to be more grounded in the work of your organization and understand Organizational holistic security
- Review of topics and tools - or engage with new ones
- Organizational Change: Make connections between topics we have covered to develop organizational policies and organizational security
- Get concrete takeaways to reinforce and deepen your understanding and practice

Reading:

Check out this workshop's section in the resources & readings chapter, to get a review of tools and ways to think about:

- Password Managers
- 2-factor authentication
- 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

W3 Homework and Practice

Practices in Organizational Holistic Security - Preparedness Assessment

Phase 1 – Foundations

Best Practices	Question	What we need to put in place to practice this
Ground in the values of the organization – policies should be aligned with the organization's values and vision so that they help an organization to practice its values. Policies should not be set that are out of alignment with or scope of the collective values and vision.	Do we have an organizational mission and vision statements? Can I facilitate a conversation about our values? If not me, who can do this? When? Where?	
Build a Team – with individuals from departments across the organization who have the authority, interest, and time to implement new security practices and policies	Who needs to be a part of this team? Can I assemble this team? If not, who can do this?	
IT Consultants/Managers/ Operations Team – engage the people who manage your IT. They will have a unique perspective on security risks and tactical approaches to reducing risk.	Who manages our IT? Can I have a discussion with them about risks that concern them and their approaches to reducing those risks? If our organization needs to implement a new tool or tactic, what is our plan for checking in with these people about implementation?	
Risk Assessment – work together to discuss risks of the work you are doing, risks to yourselves, to the people you work and organize with, to the people you serve. Discuss how people's identities and histories are linked to the risks they face. Your organizational policies should be able to support individuals who face varying levels of risks.	Can I facilitate discussions across the organization about risks individuals, the organization, and our members/ clients? Can we facilitate discussion about how different people experience the impacts of risks? Who should facilitate this?	

Phase II – Building Collective Awareness

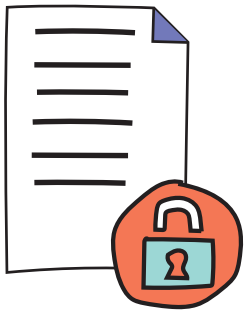
Best Practices	Question	What we need to put in place to practice this
Knowledge Building – This is making the case for security policies and practice. Build knowledge about digital security risks, tools and tactics. Make this as participatory as possible so people can see their personal and professional digital use in this.	How does my organization build collective knowledge? What spaces, meetings, bulletin boards, can we use to build knowledge about security? Who in the organization can facilitate these spaces, lead the knowledge building and sharing? What external resources will you seek, need, to facilitate collective learning?	

Phase II – Building Collective Awareness

Collaborative Policy Development – Develop policies based on what the org is already doing. Make it iterative. Separate best practices from required policies.	How can I best document current security practices? Who is the team in charge of keeping organizational policy conversations active over time? Are there opportunities for staff to evaluate and inform policy changes?	
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.	Who needs to be on the incident response team? What is the chain of communication for discussing an incident with the team? What kinds of incidents might arise and how might the team respond? How do we keep those plans up to date and make sure our staff is familiar with these plans? What agreements do we want to make about making public statements about incidents? Whose consent do we need to seek before making a statement?	
Iterate!	How frequently will we revise our safety and security policies? What incidents and events will trigger revision? What is our revision process?	

Workshop 4
PARTICIPANT WORKBOOK

Workshop 4: We do our best work when our values and practices align.



What you'll learn in this workshop:

- How to be more grounded in the work of your organization and understand Organizational Holistic Security
- Review of topics and tools or engage with new ones
- Policy and Organizational Change: Make connections between topics we have covered to develop organizational policies and organizational security
- Get concrete takeaways to reinforce and deepen your understanding and practice

Reading:

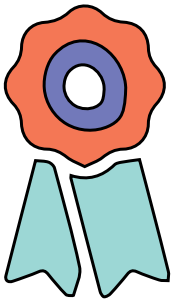
Check out this workshop's section in the resources & readings chapter, to get a review of tools and ways to think about:

- Password Managers
- 2-factor authentication
- 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

Homework:

Review a handout from a breakout group you were in and make one action plan to integrate what you learned.

W4 Homework and Practice



Aligning Values and Practices: Worksheet
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:

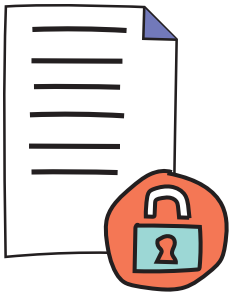
A digital practice they have is:

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?

Workshop 5
PARTICIPANT WORKBOOK

Workshop 5: Our work is ongoing, and this is the just start of a longer, sustainable process.



This workshop has another opportunity to get in-depth information on topics participants choose, and has a big section where you'll practice how you might deal with a security situation at your organization.

What you'll learn in this workshop:

- How to respond to incidents and maintain organizational security in a crisis situation
- Cultural shifts that needs to happen, not holding this work on one's own shoulders alone, how to rally teams to this work
- Do a deep dive on encryption, backups, choosing tools and safer social media practices - or other topics in an open-space breakout
- Reflect on your individual transformation as well as organizational changes throughout the course of the workshop series

Homework & Next steps:

Take this work back to your organization(s), specifically incident response planning and ideas on how to engage others.

Read the Open Space *Mini-Workshop Tool Handouts* in the Resources section to get more information from the breakout sessions' topics.

DIGITAL SECURITY READINGS & RESOURCES

DIGITAL SECURITY BACKGROUND READING

Empire, Colonialism, and the History of Surveillance

"National security surveillance is as old as the bourgeois nation state, which from its very inception sets out to define "the people" associated with a particular territory, and by extension the "non-peoples," i.e., populations to be excluded from that territory and seen as threats to the nation."
- Kundani and Kumar, Race, Surveillance, and Empire.

Racism, profiling, and the practice of surveillance are interwoven with the colonial apparatus. From the settler-colonialists so-called 'empirical observations' of First Nations peoples, designed to limit their identities to the description of them by white settlers and be used to justify the systematic dispossession of land and erasure of culture[1], to the white supremacy enshrined in the Constitution, to the modern-day profiling of racial and religious groups as [various groups of] 'the bad guys' and therefore subject to state-sanctioned harassment, scrutiny, and mass surveillance, the first step of establishing a colonialist surveillance apparatus has always been the systematic Othering of the target group(s).

Mass surveillance as we consider it today, in terms of intercepting communications, has been a practice in the States since World War I with the Black Chamber [2], a government bureau which intercepted international communications traveling through the US. Although the communications being focused on were mostly diplomatic, by the second World War, the NSA had established, for example, a mass telegraph surveillance system that collaborated with other branches of law enforcement to pass information of 'interest' to the FBI, CIA, DoD and drug enforcement agencies [3].

Further than passive surveillance, the state apparatus has been used to disrupt and harass people and groups that have not conformed to an existence gazed upon favourably by the colonial state. With the surveillance apparatus in place, 'interesting' individuals were expanded to include anti-war activists in the 60s and 70s, Black Power activists, Puerto Rican independence activists, feminists, First Nations activists such as the American Indian Movement, and other civil rights movement-builders. The COINTELPRO program 'monitored and disrupted' the lives of the above-mentioned groups, including with the use of surveillance, infiltration and soliciting informants, psychological and economic warfare (workplace interference, forging correspondence, IRS audits, false information), and violence and police killings.

Today, the state apparatus is variously targeting communities of color: Arab Americans, with widespread profiling and cataloguing (such as the 'Terrorist Identities Datamart Environment'), and state-sanctioned travel harassment initiatives towards Muslims in general, including the 'Muslim Ban'; Black Americans, with the criminalization of Black children beginning with Resource Officers in elementary schools and continuing through heightened police presence in Black neighborhoods, widespread police stops and profiling policies, and police violence; and Latinx Americans, also with disproportionate rates of police interference and youth criminalization, increased threats towards undocumented Latinx people including heightening the criminalization of undocumented families, and frequent racist rhetoric towards Mexicans being used by Trump over the course of his campaign and presidency. And this is only the tip of the iceberg, both in terms of state tactics and groups affected by these tactics.

Surveillance apparatus is not only not new, but it is also interwoven inherently with racism and identity erasure. "[P]ostcolonial racism [...] is a racism of surveillance, whereby 'foreigners' become 'aliens', 'protection' disguises 'preference', and 'cultural difference' slides into 'racial stigmatization'. [8]

However daunting this apparatus may be, strategies of resistance at this point are key to our collective strength, resistance and survival. When individual existence is a political act, groups, whose presence and realness are working against the state's identity erasure program, are revolutions, and it is no wonder that these revolutions are being met with resistance, disruption, and centuries of colonial apparatus.

First, we realize the context in which all of this is taking place, and that the surveillance we face is ingrained in the system in which we operate.

Next, we look for ways to carve out our own understanding of security in this system, by relying on our strengths and collective knowledge, and in ways that honor our own organizations and traditions.

Finally, we bring those strengths into practices which enable us to continue the work we are already doing with an increased resilience, awareness, and sense of preparedness.

ORGANIZATIONAL DIGITAL SECURITY TOOLS

Risk Assessment

Courtesy of the Electronic Frontier Foundation's Surveillance Self Defense Guide (https://ssd.eff.org/) and the Participatory Budgeting Project's Digital Security Assessment resources

Why Do A Risk Assessment?

Equity-focused organizations, especially nonprofits, and especially NPO's who work in civic engagement, lift up racial or immigration justice, or fight for voting rights or LGBTQ equality are at greater risk of scrutiny or attack in the current political climate. In our risk assessment, we will identify areas we can strengthen our preparation. A subsequent plan might look at these areas and propose ways we can change our existing practices, and develop and train staff on best practices and protocols.

An Introduction to Risk Modeling, from the Electronic Frontier Foundation (EFF)'surveillance Self-Defence Guide

There is no single solution for keeping yourself safe online. Digital security isn't about which tools you use; rather, it's about understanding the threats you face and how you can counter those threats. To become more secure, you must determine what you need to protect, and whom you need to protect it from. Threats can change depending on where you're located, what you're doing, and whom you're working with. Therefore, in order to determine what solutions will be best for you, you should conduct a threat modeling assessment.

Main Questions To Ask When Conducting a Risk Assessment

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

Additional factors to consider in your Risk Assessment:

- **Devices:** What kind of devices do you use for work or to access work material or accounts—phones, laptops, other?
- Are those devices dedicated for work only, or are they also used for personal purposes?
- Do those devices all still receive software/operating system updates? Are they regularly updated? Are they encrypted?
- **Files and data:** What kind of data do you have or produce at work? In what format? Who can access this data? What might an adversary else do with this data? Is it strictly necessary to collect or retain this data?
- **Staff:** How do staff communicate and collaborate? What kinds of software do staff use, and who controls what software is installed on any device (including phones!) that touch work data? How do staff transfer or share files?
- Does your organization have volunteers? How are they vetted?
- **Infrastructure:** Who controls wifi, networks and networked devices where you work? Do staff work remotely, from public networks, or from home?
- **Travel:** How much of your work is done while traveling? Is there a staff travel policy that contains details on what information may or may not be transported across borders or on work trips, and is there a safety plan in place for staff who are traveling? Are staff aware of this plan?
- **Other situations:** Do you have incident response/safety plans for other circumstances? Do you have plans in place for granting and revoking access to staff or individuals as their roles within your organization change?
- These are just a few of the questions that may be relevant to your organization.

Digital Security Readiness Assessment

Digital Security Readiness Baseline Assessment	✓
1. Have regular and adequate technical support provided either by staff assigned via job description or contracted with outside agencies. If your existing hardware and software are not well supported, introducing new tools and practices will likely meet with significant barriers, as new technologies and tools often demand significant ongoing technical support for proper setup and functioning. There are as many ways to secure technical support as there are organizations. Talking to peer organizations in your area is a good way to find quality help.	
2. Have a culture of training and learning, including strong technology training and follow-up as part of new staff orientation procedures. New tools and practices demand end user training. If your organization doesn't have established practices around training, implementing improved and possibly complex secure practices is nearly impossible. Beginning with documentation and training for new hires is a wise first step in this area. Following up with new employees at 30-day intervals will ensure they continue to get the support they need to do their work effectively and securely.	
3. Have a common and clearly communicated set of information systems that all staff use effectively: Know all the platforms you are using for organizational communications. If your staff are using personal file-sharing, email, task management, or other accounts without knowledge or guidance from the organization, not only will your efficiency suffer but also the environment becomes impractical to secure. How can you protect things you have no access to at an administrative level or, worse yet, don't even know are in use?	
4. Have a recurrent line item for technology in your budget. Security is an ongoing process and will require ongoing investments in computer equipment and software to be effective. Work with your technical support provider to determine an appropriate amount to put into this line item.	
5. Provide relatively new and adequately powered computers to all staff Industry standard best practice is to replace laptops and desktops every 3 to 5 years. Encryption tools use a lot of power and can bring older, inadequately powered computers to a near halt, making some security steps untenable for staff. Money for replacing 1/3 to 1/5 of your computers each year should be part of your recurring technology budgeting.	

Further Reading:

Refer to the guide at the following link for ideas on how to improve your disaster preparedness http://www.techsoup.org/disaster-planning-and-recovery.

Digital Security Readiness Baseline Assessment	✓
6. Have some baseline non-technical security practices If you do not control your office space and access to your computers, your other digital security steps can be easily circumvented by walking into your office. Rotate alarm system codes, door codes, wireless network passwords and other sensitive access procedures such as emergency building access when staff leave the organization.	
7. Make sure the computers and other devices you use, including personal devices that staff may use to access organizational information, are not compromised by malware, viruses or other intrusive software. As a first step ensure you are running antivirus software on all computers. Antivirus software for Macs and Windows computers is often available to non-profits at a discounted rate. If you haven't been running antivirus software or otherwise aren't sure about the status of your devices, you can have the operating system (OS) on it reinstalled to help guarantee the computer is free of malware and viruses. If reinstalling, use a copy from the OS provider, NOT the computer manufacturer, as manufacturers often bundle dangerous software in their installs. There are other ways in which your device can be compromised that will not be remedied by OS install. If you suspect such an issue, get a new computer and call a security professional.	
8. Have a disaster recovery plan that includes making regular backups of organizational data that are stored away from your main offices. Do not rely exclusively on third parties to back up and hold your information. This actually is a digital security practice itself, but straightforward and critical enough that it needs to come before any other digital security steps. Talk to your technical support provider about the status of your backups.	

Organizational Security and Policy Development: Coalition-building in your organization

The following are some tips to keep in mind when trying to put together a team at your organization who will examine on your digital practices and policies.

Ground your decisions values of the organization.

This can be by looking at your mission statement if you have one, or as an organization coming up with a list of values and priorities.
Include a Discovery/Research phase. In this phase, you can:

- Build your Digital Security Policymaking team, who have the authority, interest, breadth (of experience, of vocation), and time.
- Include IT providers, IT managers, or your operations and administrative team, as well as other stakeholders.
- Risk Assessment: Work together to discuss risks of the work you are doing, both to yourselves and to the people you work and organize with. Your organizational policies should be able to support your individuals who face varying levels of risks.

Knowledge-build

Build knowledge about digital security risks. Make this as participatory as possible so people can see their personal and professional digital use reflected in the stories that are told.

Political education

Some work is individual, some is organizational, and some is political.

Collaborative Policy Development

Develop policies based on what the organization is already doing. Make this an iterative process and prioritize, rather than trying to implement all changes in one pass. Separate best practices from required policies. You will need to support each other as you set short, medium, and long-term goals for your organization: do these goals consider the capacity of everyone who is being asked to make changes to their behavior? Do these goals support everyone who will be affected by these changes?

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.

Iterate

No process is complete: periodically revisit your progress, your goals, and support for the changes you are making within your organization, as well as revisiting your risk assessments, which may change due to internal or external factors. Solicit feedback from your team members who are not directly involved in your policy-making work and ask for their perspectives.

Data Stewardship With Security Mini-Audits

The Mini-audit practice:

- Identify a team, digital asset or platform, or work area to mini-audit based on your risk assessment
- Collaborate to identify issues, grounded in your values and with lots of respect for the practices of your team
- Collaborate on remediation, which may include technical and policy work, education, and practice.

Data stewardship is a caring approach to data security.

STEWARDSHIP = SECURITY

- Care-full data collection and storage: audit
- Careful use of logins: password managers, 2FA
- Careful use of internet + networks: Browsing securely, VPN
- Careful use of comms: Encrypted videos + messaging

Clarifying Data Flow What we can control vs. what we must minimize and plan for

- Let's differentiate three types of data that we interact with when we use digital devices:
- Intentional data you're flowing through your digital devices: sending an email
- Is email contents, spreadsheet contents, typing passwords private info. The goal is protecting identity info, and sensitive text (credit card #s, SSNs) in your email or browser from malicious intent, surveillance, or censorship.
- Unintentional METAdata about your digital devices: an IP address or location
- Is a proxy for you. This is the motherload of trace information that's collected about each digital user. The goal is to reduce the consumer identity data -- which companies sell, and which can be misused both intentionally and unintentionally. Also addressed here is whereabouts (IP address) masking via VPN, managing phone data, etc.
- Protected data that's within our accounts: the content of a spreadsheet
- Is only as safe as the password managing the account, or the device's password that might give access to that data, or the physical location of the device. It's also only as safe as the people using it ensure it to be, considering permissions/ sharing etc.

How we control for or minimize risk with these kinds of data:

Intentional data through your devices:

- Using HTTPS when we type in browsers to protect content from being read
- Using secure or encrypted video, chat, messaging, email
- Not typing or entering vulnerable info in the first place

Data about your device:

- Using a VPN
- keeping "location" and GPS off on your phone
- not being logged in to other platforms using Facebook, shutting down "connected apps"
- Removing extraneous apps from your phone

Protected data in your accounts

- We use passwords for our phones, tablets, and laptops
- We secure those passwords by making them strong and using 2FA where appropriate
- Keep track of digital devices, who's accessing them, and if they should be accessing them using the accounts they are (loss prevention, onboard/ offboarding)

Auditing as an Organizational Development Practice: Check in on your data with collaborative Mini-Audits

Mini-audits are great, as they allow you to do low-stakes, ongoing check ins on your team's approach, and to provide real time support to them and remediation of any issues.
A story: I did a mini-audit of an organization and asked the staff to anonymously tell me how and where they were getting on the internet, and if they had docs on their computers that weren't on our shared drive. I found that 80% of my staff used cafe and other random wifi networks regularly, and 22% had crucial documents on their computers that weren't also on our shared drive. In response I instituted fun security education emails, we put a policy in place for saving documents, and worked with IT to set up a VPN.

The Mini-Audit practice:

- Identify a team, digital asset or platform, or work area to mini-audit based on your risk assessment
- Collaborate to identify issues, grounded in your values and with lots of respect for the practices of your team
- Collaborate on remediation, which may include technical support and policy work, education, and practice.

Examples - Sit with a coworker or team, and together, try asking or exploring:

1. What's in your email? Have the team do a quick audit of email looking for things you've risk-identified. Is there any possibly vulnerable info in there?
2. Tell me how you _____ (fill in the blank based on your risk assessment or something you've noticed)
3. Do you duplicate your password?
4. Are you shopping online at work? (looking for viruses coming in)
5. How do you communicate sensitive information to members/clients/staff?
6. How do you share a file? Do you upload it to google drive/ dropbox/ use email attachments?

Protecting what you're collecting with mini-audits.

Another story: With my operations team I lead a mini-audit of our shared Drive, first just exploring permissions, and quickly learning we needed to search for "W9s" to see if we could find any out of place (we did). We moved them, changed permissions, updated our larger team, and created a new policy for saving W9s.
Planning to go forward: go over what TO do instead with your colleague or team. Practice it once together. Direct support on a password manager, strong passwords, using a VPN, checking for httpS, or installing Signal together could be here.

Examples - Sit with a coworker or team, and together, try asking:

7. Who do we share google docs with and what's in them?
8. Can you access it from "outside"? Have you ever tried to open files from outside your network? Checked permissions? Searched for vulnerable data?
9. Look at survey questions, or spreadsheets you've collected data in. You want a snapshot and to share understanding of the state of the security practices, and the tools you have at the moment.

BROWSER AND NETWORK SECURITY FOR HOW THE INTERNET *REALLY* WORKS

Browsing the Internet

What is a Browser?

Explore and learn: What are Browser settings for privacy and security?; What are trackers and cookies; Anonymous Browsing: how you do it?; When and why you might want to use this?

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 ("incognito mode"): a setting offered by most modern browsers, which involves things like deleting cookies and clearing browsing history at the end of a session (when the browsing window is closed).

This setting has nothing to do with the information that is transmitted with your http(s) requests or sent along the network; this has only to do with what information is kept locally (in your browser/on your computer) after you finish browsing.

This browsing mode is useful for: making sure other people who have access to your computer don't see your search history and can't log in to your accounts (email, social media etc.).

This setting is not useful for:

- Conducting sensitive research that you don't want traced back to yourself (by IP address, for example) consider a the Tor network and a VPN depending on your activities;
- Stopping websites from tracking you during a browsing session (eg with multiple tabs open, or in a session where you access multiple resources before closing your browser) consider browser plugins that block many trackers/cookies;
- Protecting against malicious files or phishing safe browsing/downloading practices always apply!

Trackers and cookies:

Cookies are simple pieces of data left by a visited website (and by the ads and widgets that website is running) and stored in a user's browser, often as a small text file with information about the user's behaviour on the site. Each time a user loads the site, the browser sends the cookie back to the server to notify the website of the user's previous activity. 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.

You can address a lot of web tracking with the right browser Add-ons and Extensions.

A browser extension adds functionality on to your browser, the software you use to access the internet. It can decline to store cookies, stop ads from showing, and more.

https://www.eff.org/privacybadger
https://www.eff.org/https-everywhere

Network Information, Safe Network Usage

Who manages the networks you connect to?, What do you know about them and their interests (Starbucks, airport, your organization)?

Using a network that you (or your organization) controls is different than using one controlled by a 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 on a network you don't control.

Consider the following:

- Do I know for sure if this is the network I wanted to connect to, and not a malicious network? (HotelWifi1, HotelWifiGuest, MyFreeHotelWifi...)
- Does my phone or laptop auto-connect to open wifi networks, or 'remember' networks with common names like dlink, verizonwifi, etc? (This isn't a good idea!)
- Does my laptop/phone/hard drive have file sharing enabled for networked devices? (This isn't a good idea outside the office, and might not be a good idea at all....) Related: when I connect to an untrusted network, have I marked it "Public" (on Windows) and not Office or Home?
- Do I have an older phone or laptop that has not received recent security updates and has wifi enabled?
- Do I know which other devices are on the network?
- Do I know how regularly the routers and other networking devices receive security patches and updates?

Consider adopting different internet usage habits on networks you know or control vs networks you don't. Note: most of these are good habits anywhere!

- Make sure to update your operating system and apps. Updates often fix security issues that, once known, are exploitable and important to protect yourself against. If your device runs an old operating system that does not receive security updates, it is more risky using things like Wifi and Bluetooth, especially outside a 'controlled' (home/office) environment.

- Avoid logging in to websites (such as banking, social media) on untrusted networks

- Use HTTPS as much as possible. There is a browser extension, HTTPS-everywhere, that can help with this.

- Use a VPN (see VPN section)

- Turn off Bluetooth on your phone and laptop when you are out in public (not wifi related but a good habit): https://fortune.com/2017/09/13/armis-blueborne-bluetooth-ios-android-windows-linux/

- Turn off your phone's Wifi in public if you have an older device that has not received recent security updates: https://www.wired.com/story/broadpwn-wi-fi-vulnerability-ios-android/

- Be mindful of where you're charging USB-based devices, as direct USB connections can compromise data on your device or phone. To manage this, plug a two-prong electric plug directly into an outlet rather than plugging the USB end of your cord into a USB port

VPNs: Quick how to

See full VPN Guide below in Open Space Resources

How to use a VPN in a few brief steps:

- Pick a provider [see next section];
- (probably) Sign up for a paid service;
- Create an account and download the client application (a program or app);
- Launch it and pick a server region to connect to (most VPN providers will have an 'auto' or 'fastest connection' if you don't know or don't care which region you connect to);
- Observe your IP address change by going to https://whatismyip.com and/or make sure you're properly set up by going to https://dnsleaktest.com/
- Happy browsing!

Internet Infrastructure: ISP and a National Gateways

An Internet Service Provider (ISP) is a company (or organization) that provides services for accessing the Internet. Internet service providers may be commercial, community-owned, or non-profit, but typically they are private companies (such as Verizon, Comcast, AT&T in the USA).

When you make a web request, your request is first resolved to an IP address*, which is a public address. Your router sends this address to your ISP, which forwards the request to the ISP of the service you want to access, and the response is sent back to your ISP then to your router and finally, to your device. So, your ISP is an essential intermediary in sending out your requests and retrieving and your content as you browse the internet.

*The way this address is 'resolved' is by using domain name servers (DNS), which translate the url you have requested into an IP address and vice-versa. There are different DNS servers—usually the ones you use are assigned by your ISP, although it's possible to change which ones you use, usually by changing configurations on your router.

So, an ISP being a part of the chain of your internet use 'knows' what sites and services you (and their other clients) are requesting access to, and also knows your payment information (name, billing address, etc.) because they are a service you pay for. In the US, ISPs are subject to FCC regulations on privacy, however, recently, these regulations changed to allow ISPs much more leniency on how they treat your data. In fact, ISPs face less regulation around selling your data to

3rd parties, and now there is also the risk that ISPs or internet hosting companies can be requested/required to hand over customer data (see further reading).

For these reasons, it is important to consider the nature of your internet usage. Are you Googling or researching sensitive terms or accessing sensitive material that you would not want traced back to you? You should not necessarily consider information your search for or access to be "private," unless you are taking steps such as using a trusted VPN (see next section) to access web content.

A National Gateway is a router that serves as an entrypoint for the internet in your country. Internet traffic to and from any device passes through the national gateway as it is being routed to your device from the internet. Therefore, in the national gateway is also a place at which internet traffic can be (and is) monitored.

Some countries are more widely known for blocking content nationally, such as Iran, which blocks a wide variety of Western media and platforms such as Twitter, as well as Iranian content that is seen to be contrary to the regime or its morals, and China, which is known for the so-called "great firewall," blocking certain search terms, websites, emails, and severely filtering and monitoring content access. But national level monitoring and censorship programs exist worldwide.

The OONI (Open Observatory of Network Interface) project is a project that monitors internet access around the world, conducts tests on blocked content, and provides reports on internet health and access. https://ooni.torproject.org/

OPEN SPACE TOOL HANDOUTS

Phishing and organizational culture!

An important way to make phishing attacks even less likely to succeed is to make them stand out--that is, to make them look so bizarre/unusual that it would be hard to just fall for one when you're tired/busy/rushed. What does this look like? This means having agreements and practices in your organization that allow you to avoid 'phish-y' behavior in your day-to-day interactions.

However, what do we do when we get that email from our boss that says "Urgent please respond asap: http://goo.gl/BitGdu78c ?" For our digital security strategies to really be effective, we need a culture in place where we encouraged to check in if we aren't sure about something, no matter whether we are talking to a supervisor, a new employee.

In this case, **verifying off-band** (checking in in another modality, such as in person, text message, etc) is a great way to a) make sure the correspondence is legitimate, b) gently remind each other that this kind of communication makes us all more vulnerable when attacks come along.

Perhaps you decide on certain practices in your organization; for example, some such practices around email hygiene might be:

- a 'no clickbait' policy-- (never sending one-liner emails like "check this out!!: http://my.cool.link"), or
- deciding not to use URL shorteners at all (*can you think of why?), or
- always typing links in an address bar instead of clicking through on them with emails (*can you think of why?), or
- a 'no attachments'/'careful with attachments' policy

Are there any policies like that you could bring back to (or dream up with) your organization? There is a 'policy bingo' activity for some possible policies or practices. Not all are related to phishing. Feel free to create your own policy bingo as well.

When are we most vulnerable to phishing?

- Around holidays or other busy, stressful times (or times when we may be encountering a lot of online interfaces that we don't typically encounter, such as increased online purchasing, travel booking, etc)
- A targeted attack might come in the weeks/days leading up to an important internal milestone: a big project, an election, a funding deadline
- When we're stressed/tired
- When we're not paying attention
- When we feel social pressure/when it seems urgent

Add to this list and keep track of when you're most vulnerable--as an individual, as an organization--and pause to consider the source and situation before taking any action, especially around texts or emails.

Encrypted Video Calling (Alternatives to Skype!)

One of the major revelations of the Snowden leaks was that companies like Microsoft (and Facebook, Google, Apple, etc) comply with PRISM requests for data from Skype, Outlook.com, and Skydrive, and specifically help the FBI and CIA bypass encryption and access data from these sources. (To read more about PRISM, see "further reading" below).

In particular for sensitive topics, but really for any topics, we don't need 3rd parties or government listening in on our chats or video calls.

Let's look at options other than Skype for video calling.

What makes a good alternative:

Consider your needs. You may find options that fit some but not all of your needs—this is a good chance to make a chart that can help you figure out what each platform offers. We can put criteria (your needs) at the top, and see how our options measure up. This is useful in many scenarios when trying to evaluate a new tool.

In general, we are looking for an encrypted solution, meaning essentially that the intermediaries that transmit your data can't read your data.

We may also be looking for other features (does it work on my phone/laptop? Do I need to create an account?), and we can organize those needs into a chart. Here is an example of such a comparison:

(and more: Ring (https://ring.cx/), Tox (https://tox.chat/), tokbox (https://tokbox.com/), Linphone (https://www.linphone.org/)

Name	E2EE?	Free	Supports Groups?	Supports my device?	"Easy" to use?	Other criteria?
Jitsi	Y	Y	Y	Y	?	
Signal	Y	Y	N	Android/ iOS + MS/Apple/ Debian	Y	Tied to #
Silent Phone	Y	N	Y	Y	?	
WhatsApp	Y	Y	N	Y	Y	Privacy concerns
Appear.in*	N	Free/ paid	Y	N	N	Platform concerns

Encrypted Messaging using Signal or WhatsApp

Why not just regular text?

SMS (regular text messaging) is built on an old protocol, and is vulnerable to interception. Your text messages could be intercepted by skilled individuals or by government, and you should not consider the contents of text messages to be private. (This is also why SMS is not an ideal method of authentication in 2-step authentication).

To send messages that cannot be readily intercepted by 3rd parties, consider using a messaging app that offers end-to-end encryption (E2EE).

Alternatives to SMS: Encrypted Messaging

Both WhatsApp and Signal are apps that offer end-to-end encryption.
Note that non-SMS-based messaging systems like Signal and WhatsApp require data or a wifi connection to send and receive messages and calls, and sender and recipient have to be on the same app (I can send encrypted messages on Signal to other Signal users).

Signal carries your encrypted messages from your device to the recipient's device through their own servers, but they cannot read the messages, and messages are removed from their servers after they are delivered. Signal is specially designed to be as minimal about metadata as possible, and removes most records of a message after it has been delivered (see further reading). Signal is like text messaging in that it requires a phone number to set up.

WhatsApp is owned by Facebook and requires a Facebook account. WhatsApp uses the same encryption protocol as Signal, meaning Facebook cannot read your private Whatsapp messages, but using WhatsApp creates a link between your other Facebook activities and your WhatsApp activities. WhatsApp has a Windows phone app, while Signal does not.

Although you can currently opt out of some data-sharing between Facebook and WhatsApp, Facebook or a government entity cooperating with Facebook can still see who you're sending messages to, what time they were sent, and make inferences about what you're up to based on other Facebook activities (such as event RSVPs, likes, and common friends in your or your recipient's "social graph").

Safer Social Media Use

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.

It can be helpful to take a *harm reduction* approach to using social media. It's not realistic to cut off cold turkey, but there are steps you can take to help mitigate risks to you and/or your organization.

Remember that if/how/when your organization uses social media depends on your *risk assessment* - which can change over time and depending on the platform.

Here are some questions to consider when using social media:

- Do I use the same social media handle(s) for work and personal? Do I use my real name or register with my primary email address? Consider using a separate email address that doesn't have your name or any identifying information in it to register for accounts
- Have I checked my privacy settings, and am I aware of who can see what I post, or which people or groups I'm connected to?
- What information might my contacts be able to pass on about me, and vice versa? What if one of our accounts was compromised?
- Do I have a strong password and have I enabled 2-factor authentication on my social media accounts? Be thoughtful when choosing a password! https://www.youtube.com/watch?v=opRMrEfAIiI
- Do I have account recovery questions that are 'public' or searchable information (for example, my first pet's name, my hometown, etc) that I may have put on social media? (Avoid this!)
- Do I share things that could put me in at risk if my family member, acquaintance, employer, or other authority were to see them?
- What else am I sharing when I'm posting? For example, the time of day that I post, my location, pictures of my house, family, or neighbourhood, metadata from photos or videos I post or media of me, etc. It might be wise to turn your location services off.
- What, if any, 3rd-party apps have permission to access my accounts (for example, a productivity app that wants to access my Google Calendar)?
- Do I post pictures of my face/identifying features on social media, and/or do I use pictures that I have used elsewhere online? Note that reverse image lookups via Google can be used to link profiles.

Safer Social Media Tactics/Practices

- Consider having separate accounts: you may not want to share sensitive content or perform work-related activism from accounts where you (have pictures of your face, your family, list your job or city, etc)
- Consider the extra information that says a lot about you: do you need to link your family, significant other, school, or job? Do you need to tag photos with people and locations?
- Consider your privacy settings and whether you can have friends-only, followers-only posts
- Consider another modality for sharing information: mailing lists, phone calls, encrypted chat groups, in person/offline
- Consider all information posted on social media to be potentially publicly available. If that doesn't feel safe, find another way to disseminate that information.
- If you're sharing a video or photograph on social media and need to protect anyone's identity (and remember tattoos, clothing can also be markers of a person's identity), try using Youtube's free blurring tool to anonymize them. But make sure to edit from a copy.

Tutorial here: https://blog.witness.org/2017/08/introducing-youtubes-updated-blurring-feature/

Action Safety Planning

How can we better prepare to protect ourselves, our data, our devices, and communications before an action? What might we want to protect?

Tactical tips to protect...

Phones
- Lock using a 6 digit passcode, not pattern lock or fingerprint ID
- Delete any sensitive information – contact numbers, notes, texts, etc.
- Memorize importation numbers (legal contact, trusted organizer, etc.) or write on your arm
- Make sure you have enough space if you are documenting
- Back up footage to the cloud in case your footage gets deleted or your phone confiscated, but beware that this could potentially tie you to an action/location in case you are trying to be anonymous
- Are location services turned on? Do you want them to be?

Social media accounts
- Are you posting from your personal account? Does it have location information?

Communications
- Use Signal – turn on disappearing messages
- It's important not to just rely no tech for safe communications. Have plans come together in person when possible. Have community contracts. TRUST and community-building is how we stay safe!

Questions to Ask Yourself

If you have decided to go ahead with your action, begin answering the following questions about your resources.

- Do others know where I am going? Are there people who are not at this action who know when/where to check in with me and my anticipated return? Is there a plan if I do not reach them at the scheduled time?
- Do I have important information (such as emergency contacts) memorized or written on my body?
- Have I made a list (inventory) of my equipment and everything I am carrying, including photos, and shared it with a trusted friend/lawyer/ally?
- Do I know the area I am going to, and my transportation options?
- Am I prepared physically (clothing, nutrition, footwear, first aid, or other gear appropriate to situation)?
- Do I have a plan for what I will do with any documentation/film I may get?
- Am I carrying anything I don't want to be carrying (valuables, specific pieces of ID) or wearing clothing that might identify me in ways I don't want?
- Is anything I am carrying or bringing, including my media equipment, going to impair my ability to run or move quickly?
- Am I part of a team, or am I alone? If part of a team, do we have roles in this action, ways of communicating with each other, and backup meeting place/plan if we cannot communicate?

Filming/Documenting Safely

Before choosing to document your action, conduct a Risk Assessment.
Here are some questions you may want to include:

- What am I going to document? Who might be affected by my actions? Am I familiar with this group, cause, or situation?
- Can I afford for my equipment to be lost, seized, or damaged?
- Is it likely that I will be interrupted, and if I am, am I prepared for the consequences (for example, will I be arrested, is there money for bail, can I miss the next workday, is my immigration status an additional factor to consider, (how) will others be affected if I am stopped)?

Here are some essential pieces of information on documenting/filming things in public (such as protests or police action) in the US.

You may legally film police, as long as you comply when told to back up.
Your equipment (phone, camera) can be confiscated, and if it is unlocked biometrically (e.g., a phone with a touchscreen password), you can be compelled to open it. However, you cannot be compelled to give up your PIN or passphrase if it is not biometric.

Important Action Plan:

You should consider whether there are people at this action who would be endangered if they appeared on film.

Tips on effective filming and documenting:

- Document the date (film a newspaper, or say the date), street signs, and other location information
- Document badge/ID numbers and other details
- Try to film continuously, in particular with events like arrests
- Film from a "safe" angle, try to capture multiple angles as well as details
- Film deliberately, and try to use smooth movements and longer (10s+) shots for clarity

After you have documented:

- You will need to securely store backups of your footage.
- Make sure to preserve a copy of your original unedited footage
- Make sure to again consider the implications for others who were caught on film—did they consent to being filmed? Could they face any consequences for having been filmed?

Further reading on Protest and Action Safety Planning:
https://library.witness.org/product-tag/protests/
Filming ICE tip sheet - https://witness.org/filming-ice/

Virtual Private Network (VPN) Deep Dive

What is a VPN?

A VPN (Virtual Private Network) is a service that lets you create a connection to another network over the internet—ideally, a secure and encrypted connection. What this means in practice is that, if you were to monitor the internet traffic (web requests and responses) from your computer or phone, instead of seeing connections to a variety of sites and services online any time you browsed the web or used an application that needed internet, all your connections would be to the VPN provider.

The easiest analogy to describe a VPN is as a "tunnel"--you connect at one end, your requests are handled at the other end, but the traffic in between is encrypted and therefore not visible to intermediaries.

VPN providers, which are companies that offer this as a service, will have a range of servers around the world that you can choose to "tunnel" your connection through—for example, your are connecting to the internet in New York City, but you connect to a VPN server in Belgium, and now your IP address appears to be from Brussels.

Further reading:
https://thatoneprivacysite.net/vpn-section/
https://www.privateinternetaccess.com/pages/how-it-works/

How to use a VPN

Most people will sign up for a service, perhaps from this VPN Shortlist or another provider.

- Private Internet Access: https://www.privateinternetaccess.com/pages/buy-vpn/
- TunnelBear: https://www.tunnelbear.com/
- VyprVPN: https://www.goldenfrog.com/vyprvpn/

Alternately, some browsers offer internal VPN services.

- Before you connect to any website, turn on the VPN
- Then, browse as you planned to otherwise

Why you might use a VPN

Privacy from your ISP.
ISPs connect our computers to the internet and without a VPN, have a record of all the activity we do on the internet including sites we visit, web services we connect to and a slew of metadata about this activity. https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections

Nefarious Website Owners.
Sites and services we visit see linked to our IP addresses. Are you visiting sites and services that you don't want linked to an IP address that can be linked to you personally?

Nefarious Wifi Operators.
The first step your internet communication takes from your computer is across your network (wireless or wired). Your network, like your ISP can see the sites and services you visit linked to our IP address. Do you want the network operator to create and keep a record of this? (Hint: no!) http://www.slate.com/blogs/future_tense/2016/11/02/don_t_connect_to_public_wi_fi_anywhere_you_wouldn_t_go_barefoot.html

What doesn't a VPN protect you from?

Some things VPNs don't protect us from:
- Trackers/cookies (use browser plugins like Privacy Badger, uBlock to mitigate being tracked)
- Phishing, malware, suspicious websites--the same safe browsing/safe downloading rules always apply!
- Whatever information the VPN collects--we're trusting it the way we would trust our ISP

When might my VPN not work?

(See: "What doesn't a VPN protect me from?" section, above)

- If you are in a country where VPN use is being blocked (https://en.wikipedia.org/wiki/VPN_blocking)
- If you are trying to access a service that blocks VPNs (for example, Netflix and other streaming services)
- Technical difficulties: connection/routing issues
- Some (older) protocols can be blocked by your ISP (such as PPTP), but not newer ones (OpenVPN)
- If you are exposing your private data in other ways

How do I choose a "good" VPN?

As seen in previous sections, your VPN will know a lot about you and your browsing habits, as your ISP would, and so it's important to understand a) their business model, and (related) b) their motivations for providing this VPN service.

As with most free services, remember the following:
- If it seems too good to be true, it probably is.
- If you're not paying for the service, you may be the product.

What does that mean? Personal data is valuable, and if a VPN provider is not charging for the service, they may be monetizing client data (by logging your traffic, user patterns, etc).

Any software/application has to keep some logs; if something in the application is broken, logs are how the people maintaining the app or service know what to fix. But there are different types of logs, different ways to keep logs (for example, aggregating and anonymizing vs storing separate logs on individual users, deleting logs after a certain time period, having a minimal logging policy etc).

Additionally, remember that a VPN can provide you with privacy (others can't necessarily observe your browsing) but not total anonymity (someone, i.e. the VPN provider, still knows what you were looking at and when.) Total anonymity is not a realistic goal or promise, and any company that claims to offer that is not accurately representing their service—some data collection that does de-anonymize is required to keep services like VPNs running.

So, some things to look for in a VPN provider:

- Are you paying for the service? This is a hint that they have a sustainable business model and aren't just monetizing your data.
- Do they clearly state their logging policy in detail?
- Has this logging policy been tested—for example, has the VPN been subpoenaed for user records, and what did they provide? Did they or others publish anything on this occurrence?
- General reputability: do they make hyperbolic claims like "Ultra-secure, zero logging, total anonymity online" etc? These claims are suspect, and are generally contraindicated in the fine print.
- Peer review: has the VPN had their code audited or been reviewed? Did it happen recently?

Some other criteria that may affect your choice:

- Does the VPN offer "multi-hop" connections as well as "single-hop"?
- Does the VPN application support all of my operating systems (laptop, phone)?
- Does the VPN application offer the ability to disconnect/block all my internet connections until I am securely connected via VPN, to prevent IP leak for example when the computer or phone is starting up?

When using a VPN what of my internet use is visible and what is not?

- First of all, this information applies if your VPN is configured correctly, meaning that you have checked https://dnsleaktest.com/ or similar and aren't leaking your IP address. More on that in a minute.

Think of the internet diagram from workshop 2.

To people looking at traffic on your network: all your connections will appear to be going to one IP address*, representing the server you connected to with your VPN app. This will be an IP that is connected to the region you chose (so if you picked 'connect to France', your IP might be from Paris.) It will appear that you are using the internet in Paris.**

Caveats:

- This IP might not be the same all the time; sometimes you will have a dynamic (changing) IP address, but there should be only one IP at a time during your connection.

- If you have cookies or browser trackers that stored information from before you connected to your VPN, you may still find that your browsing experience is more like an American user who happened to take their laptop to Paris—e.g., your Google results are still in English despite your connection appearing to originate from France. This just means that there are multiple factors that contribute to being 'identified' on the internet, and IP address is only one of them.

To your ISP:
The situation will be similar to those looking at traffic on your network. They will be able to see outgoing and incoming connections to the one IP address elsewhere, and because of this traffic pattern, they will be able to identify that you are using a VPN. (As would someone observing your local traffic.) However, the requests would be encrypted, so that they would not be able to see which sites or services you were visiting/using.

To your VPN Provider:
Because your VPN provider is responsible for handling all your requests, they must be able to see which sites/applications you want to visit/use and provide (serve) content from those sites or applications. This means that your VPN provider is essentially in the role that your ISP was in before—they see what content you are accessing and when, with the same limitations of any ISP (for example, recall the difference between sending http and https requests).
This means that knowing your VPN provider and the kind of data they keep on their users is extremely important. [see next section.]

Further reading:

- https://thatoneprivacysite.net/vpn-section/
- https://www.expressvpn.com/what-is-vpn/policy-towards-logs
- The impossible task of creating a "Best VPNs" list today
- https://arstechnica.com/information-technology/2016/06/aiming-for-anonymity-ars-assesses-the-state-of-vpns-in-2016/
- Remember: with a VPN, you are obtaining privacy, but not necessarily anonymity! (https://www.privateinternetaccess.com/blog/2013/10/how-does-privacy-differ-from-anonymity-and-why-are-both-important/)

Two Factor Authentication

What's 2 Factor Authentication?

It's a more secure way of logging in, involving something you know, and something you have. In this case, a password is the thing you know, and a token of some sort (on your phone, or a physical hardware token) is the thing you have.

Why should I use it?

If your account credentials are compromised (in a phishing scam, a data breach, etc), an attacker still can't log in to your account without the second factor—it's extra protection and helps keep your accounts secure.

What kinds of 'second factors' are there?

From best to least-preferable: a hardware token (like a Yubikey or Nitrokey), a token-generating app (Authy, Google Authenticator), and SMS-based (getting a text with a number code). You will also find some services (such as banks) offer a phone call or an email as a second 'step' for authenticating, which may be better than nothing but are still not as good as another method.

How does it work?

- If the platform you are using supports 2FA, get an authenticator app or hardware token (you may need both—many services support an app as a second factor, but support for hardware tokens is still growing).
- Follow the instructions to set it up with your account (Gmail, Twitter, Facebook, AWS, Github, and many more services support 2fa: see a list at https://twofactorauth.org/ or check your platform/service's website).
- During setup, you will 'pair' your account with your second factor, and from then on, you will be asked for both your password and your second factor when you log in.
- If you are given the option to download 'backup codes,' do so! These one-time codes are an extra way of logging in, if you lose your phone or key somewhere. Store these codes in a safe place (a safe or a password manager or both).

What if I lose my phone/key/I uninstall my authenticator app?

If you don't have backup codes, this can lead to you getting locked out of your account—it's important to keep backup codes somewhere safe for this reason. Different platforms may have different account recovery mechanisms. Don't uninstall your authenticator app while you still have 2FA enabled.

Read more on 2FA: https://twofactorauth.org/

Passwords and Password Manager Review

What happens when we reuse passwords/passphrases?

Reusing passwords puts us at risk of compromise. Data breaches are common (check out https://haveibeenpwned.com/), and if we use the same or a similar password and it is compromised on one account, our other accounts become that much more vulnerable.

Even changing a few characters of a password doesn't protect us that much—if your passwords are at all similar to each other, you are more vulnerable to attack.

What's a "good" passphrase?

Long, unique, not made up of personal information, and strong (a mix of numbers, letters, characters). Length is very important—a short password does not take very much time for a computer to crack (called "brute-forcing"). A good password should not contain anything that's relevant about you: no birthdays, pet names, favourite ice cream, or lucky numbers.

But...how do I keep track of all these long, strong, unique passphrases?

Our suggestion is to use a password manager: a piece of software that stores your (encrypted) passwords (and can do other things, like store secure memos, generate a long strong password for you when you open a new account, etc). If you use a password manager, the only password you remember is the "master password"--the one that unlocks your access to all your other passwords. There are different kinds of password managers—online and offline—and there are some with apps that you can use on your mobile device as well.

What are some password managers you recommend?

We currently recommend LastPass (https://www.lastpass.com/) and 1Password (https://1password.com/) due to their combination of convenience and security, although there are many online and offline to choose from and we don't all use the same tools ourselves.

Trusting a password manager: why?

This is a common question. Security professionals believe that it's safer to trust a reputable password manager that has been through security audit(s) and been subject to tests and scrutiny than it is to rely on a small, short password you keep in your head, or on a password that you reuse. The fact is that for a password to be strong enough these days, it's pretty much not something you can memorize, let alone memorizing many of them (for your banking, email, social media... and more).

If you are a very high-profile target, and you feel that your attackers might include government who would target you specifically, read the next section, "Do I have to use a password manager?".

Do I have to use a password manager?

A password manager is a means to an end. If you feel unsure about the idea of a password manager, ask yourself: do I have a secure and private means of storing many long, strong, unique passphrases, and making sure my passphrases for all my accounts are unique and random? Are there some passwords/passphrases I would be comfortable storing in a password manager (perhaps for less sensitive accounts)? Would I feel safer if I used an offline password manager (basically, having an encrypted database on your computer) instead of an online one? Are there a few passwords I will make it my priority to memorize?

The bottom line is, your security strategies need to keep you and your organization safe, and there are risks to (for example) writing your passwords down on paper, reusing your passwords, or picking short or 'relevant' passwords that an attacker could generate based on information about you. We (as trainers) use a combination of online and offline password managers to meet our security needs. Be informed about the risks and benefits of different options, and conduct your own risk assessment to determine what's right for you, just make sure your passphrases are long, strong, and unique, and cannot be accessed unexpectedly by others.

In any case, you should turn on 2-factor authentication for as many services as possible, so that no matter what your password decisions are, you have the added security of a second step to log in.

Further reading on passwords: https://ssd.eff.org/en/module/creating-strong-passwords

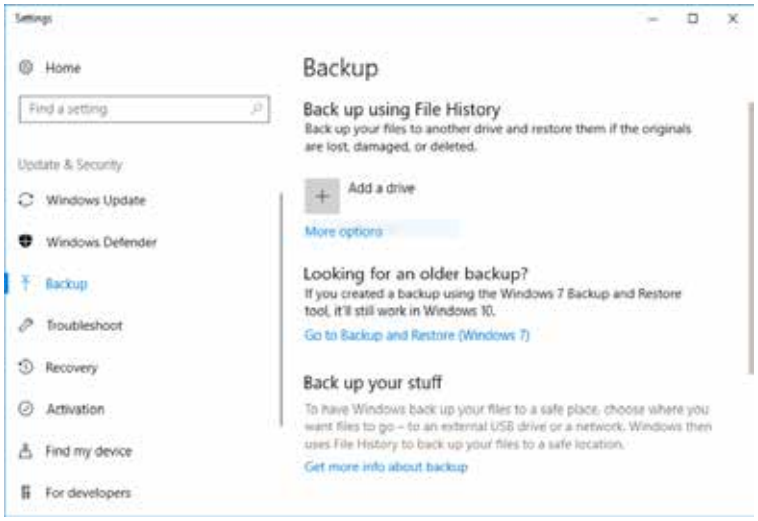
Safer Backups

Backups in Windows 10

Windows 10 includes a built-in backup utility in Settings > Update and Security > Backup. Under "Backup using File History", you can choose an external hard drive (the larger the better, at least 1TB+ if possible) to back up to.

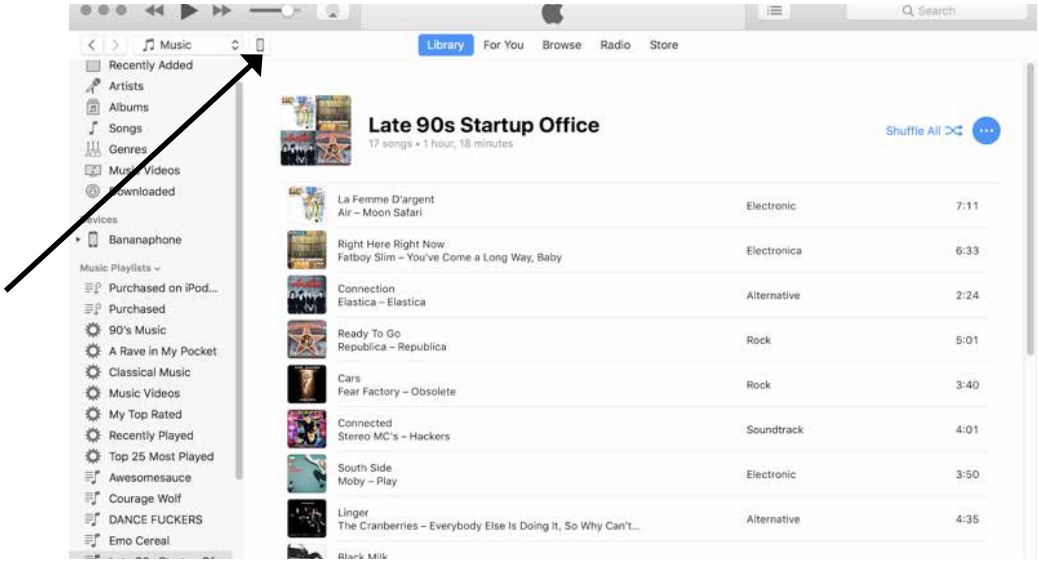
NOTE: Windows does not encrypt the drive automatically. For encrypted backups on Windows, you can use a paid end-to-end encrypted backup service such as Spider Oak's Backup One (https://spideroak.com/one/).

See https://support.microsoft.com/en-us/help/17143/windows-10-back-up-your-files for more details.

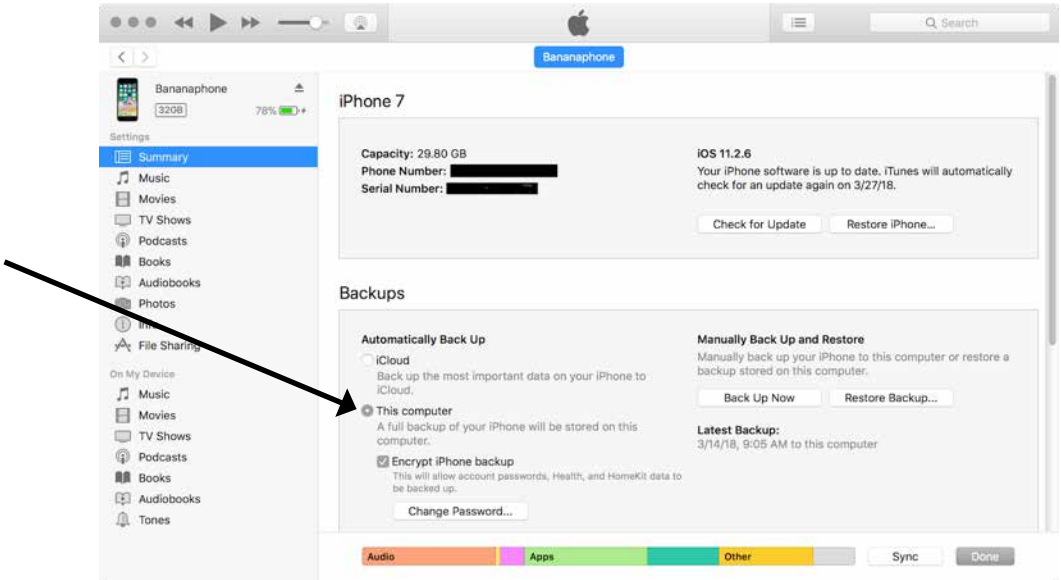


Backups - in Mac & iOS

When you plug in your iOS device to your Mac, you can use iTunes back those up, which also happens automatically any time you sync your iOS devices with iTunes. Click the phone icon in iTunes to get to the device's sync settings.



These backups can be encrypted, but make sure to use a strong passphrase to encrypt them with, and keep that passphrase stored safely in a password manager. Encrypt your backup to your computer instead of iCloud to keep your backups offline.



Backups in macOS

Time Machine is a free backup utility included on all recent versions of macOS. You can backup to an external hard drive (the larger the better, at least 1TB+ if possible), and encrypt the drive with the same kind of full-disk encryption used to protect your Mac's hard drive. Once you connect your external hard drive, macOS will ask if you want to use it for Time Machine and if you want to encrypt it. Check the option to encrypt the backup disk and click Use as Backup Disk.
The added bonus is that if you have been backing up your iOS devices with iTunes, the backups for those devices also get backed up with everything else on your Mac.

See: https://support.apple.com/en-us/HT201250 for more details..

FURTHER READING

Read more and get a PDF of the full Stronger NYC Communities *Digital Security Guide* at https://strongercommunities.info

There have been several comprehensive guides on learning about digital security, data collection, and protecting yourself or your information, published by reputable organizations, and they are our first recommended reading. They include:

The Electronic Frontier Foundation (EFF)'surveillance Self Defence Guide (https://ssd.eff.org/, in Spanish at https://ssd.eff.org/es), as well as their Security Education Companion Guide (https://sec.eff.org/)

Hackblossom's DIY Guide to Feminist Cybersecurity (https://hackblossom.org/cybersecurity/)

The variety of guides and toolkits from Tactical Technology Collective (https://tacticaltech.org/projects/toolkits-guides/), including Security in a Box (https://securityinabox.org/en/), which is translated in Spanish here (https://securityinabox.org/es/).

Citations and Further Reading on the History of Surveillance

[1] Arun Kundnani and Deepa Kumar. Race, Surveillance and Empire. International Socialist Review 96, https://isreview.org/issue/96/race-surveillance-and-empire.
[2] https://en.wikipedia.org/wiki/Black_Chamber
[3] https://en.wikipedia.org/wiki/Project_SHAMROCK / https://en.wikipedia.org/wiki/Project_MINARET
[4] https://www.democracynow.org/topics/cointelpro
[5] John W. Whitehead, A Government of Wolves: The Emerging American Police State
[6] Justin Leroy, Black History in Occupied Territories: On the Entanglement of Settlement and Colonialism, https://muse.jhu.edu/article/633276
[7] Alfred W. McCoy, Policing America's Empire: The United States, the Philippines & the Rise of the Surveillance State.
[8] Huggan, Law. Racism Postcolonialism Europe. https://liverpooluniversitypress.co.uk/products/60819
[9] Mahmood Mamdani, Define and Rule: Native as a Political Identity. https://www.amazon.com/Define-Rule-Political-Identity-Lectures/dp/0674050525

Further Reading on Browsing and Wifi:

Risks of using public wifi:
https://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/

Bluetooth malware:
https://fortune.com/2017/09/13/armis-blueborne-bluetooth-ios-android-windows-linux/

Starbucks Wifi is designed to make money off of you: https://www.forbes.com/sites/rogerdooley/2013/10/11/starbucks-wifi/#60939421ddc1

EFF Tools to Protect Yourself Online: https://www.eff.org/deeplinks/2016/09/five-eff-tools-help-you-protect-yourself-online

Further reading on Internet Infrastructure:

Censorship and national gateways https://www.theguardian.com/commentisfree/2008/nov/10/internet1

What is an ISP https://www.lifewire.com/internet-service-provider-isp-2625924

ISPs and your data https://www.forbes.com/sites/thomasbrewster/2017/03/30/fcc-privacy-rules-how-isps-will-actually-sell-your-data/#28911b0c21d1

ISPs and FCC regulations http://www.techradar.com/news/2017-isp-privacy-regulations-in-the-united-states-all-you-need-to-know

Internet hosting companies being subpoenaed http://thehill.com/policy/cybersecurity/346544-dreamhost-claims-doj-requesting-info-on-visitors-to-anti-trump-website

Internet shutdowns https://www.apc.org/en/blog/internet-shutdown-gambia-our-story – a great 1st person account from a colleague about the 2016 shutdown in Gambia

http://www.pbs.org/wnet/need-to-know/the-daily-need/could-our-government-shut-down-the-internet/6975/

Internet censorship https://learn.equalit.ie/wiki/Internet_Censorship

List of internet exchange points (IXPs) https://en.wikipedia.org/wiki/List_of_Internet_exchange_points

Viewing and reporting sites that are blocked around the world, in real time: https://www.herdict.org/#

In-depth chapter on internet surveillance and monitoring: https://equalit.ie/esecman/chapter2_5.html

Mathias Klang, Andrew Murray. Human Rights in the Digital Age. Psychology Press, 2005. 243 pp.

Censorship and national gateways https://www.theguardian.com/commentisfree/2008/nov/10/internet1

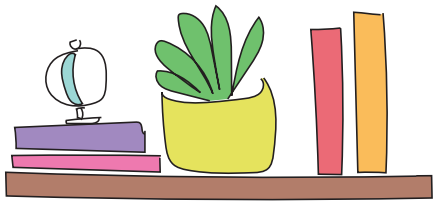
ISPs and your data https://www.forbes.com/sites/thomasbrewster/2017/03/30/fcc-privacy-rules-how-isps-will-actually-sell-your-data/#28911b0c21d1

ISPs and FCC regulations http://www.techradar.com/news/2017-isp-privacy-regulations-in-the-united-states-all-you-need-to-know

Internet hosting companies being subpoenaed http://thehill.com/policy/cybersecurity/346544-dreamhost-claims-doj-requesting-info-on-visitors-to-anti-trump-website

Internet shutdowns https://www.apc.org/en/blog/internet-shutdown-gambia-our-story – a great 1st person account from a colleague about the 2016 shutdown in Gambia

http://www.pbs.org/wnet/need-to-know/the-daily-need/could-our-government-shut-down-the-internet/6975/



Further reading on browsers and tracking:

https://myshadow.org/browser-tracking
https://www.whatbrowser.org/
https://www.eff.org/privacybadger
https://www.eff.org/https-everywhere
https://www.torproject.org

Further Reading on safer use of Wifi:

Risks of using public wifi: https://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/

How Starbucks Wifi is designed to make money off of you: https://www.forbes.com/sites/rogerdooley/2013/10/11/starbucks-wifi/#60939421ddc1

Firesheep (2010 story) http://money.cnn.com/2010/12/14/technology/firesheep_starbucks/index.html
http://codebutler.com/firesheep?c=1

Further reading on Encrypted Video Calling:

https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

Further reading on safer SMS and messaging:

- Signal's low data collection policy as tested by a subpoean: https://signal.org/bigbrother/eastern-virginia-grand-jury/
- Phone numbers are how you identify people on Signal, so it's important to verify the phone number of the person you're chatting with:
- https://support.signal.org/hc/en-us/articles/213134107-How-do-I-verify-the-person-I-m-chatting-with-is-who-they-say-they-are-
- Opting out of WhatsApp add-tracking on Facebook (note that you cannot opt out of all data sharing between WhatsApp and Facebok): https://faq.whatsapp.com/en/android/26000016/?category=5245250

Further reading on Protest and Action Safety Planning:

- https://library.witness.org/product-tag/protests/
- Filming ICE tip sheet - https://witness.org/filming-ice/
- Checklist: Sharing Videos of Encounters with ICE - https://library.witness.org/product/checklist-sharing-videos-of-ice-encounters
- https://www.aclu.org/other/fighting-police-abuse-community-action-manual#organizing
- http://www.berkeleycopwatch.org/
- https://www.eff.org/deeplinks/2016/11/digital-security-tips-for-protesters
- https://ssd.eff.org/en/module/attending-protests-united-states

Comprehensive online guides on safer social media use:

Security in a Box https://securityinabox.org/en/guide/social-networking

Surveillance Self-Defence Guide: https://ssd.eff.org/en/module/protecting-yourself-social-networks

Checklist: Questions to ask yourself before you share a video on social media https://library.witness.org/product/checklist-sharing-videos-of-ice-encounters/

Opting out of data brokers on Facebook: https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook

CONTENT GUIDANCE
GLOSSARY

2-Step Verification / 2-Factor Authentication (2FA), a process that requires multiple factors to access information, an account, etc. 2FA usually requires a password, username, and another piece of information that a person has physical access to like a code sent to email, a phone, or generated by a software token or hardware token.

Administrative Access, a level of access to a system that allows a user to make major changes to a system and has greater access than a normal user. The types of changes vary based on the system. A administrator on a computer typically has access to install and uninstall applications. An administrator on an account based system typically has access to create and delete accounts.

Authenticator Application, a type of software token, often an app run on a mobile or desktop device, that generates 2-Step Verification authentication codes

Biometric Verification, any means by which a person can be uniquely identified by one or more biological aspects for example, fingerprint, retina patterns, voice waves, DNA.

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.

Browser extension / Browser plugin, a piece of software that extends the functionality of a web browser. Examples include HTTPS Everywhere, Privacy Badger.

Cookies, also called **HTTP/Web/Browser Cookies,** Trackers, are simple pieces of data left by a visited website (and by the ads and widgets that website is running) and stored in a user's browser, often as a small text file with information about the user's behavior on the site. Each time a user loads the site, the browser sends the cookie back to the server to notify the website of the user's previous activity.

Data, digital information, e.g. a password or a file.

Data Backup, a copy or archive of files and data created for the purpose of restoring data in case of loss from risks like hardware failure, loss or theft, computer viruses, file corruption.

Digital Privacy, appropriate and adequate protection of personal information shared on digital networks.

Domain Name / URL (Uniform Resource Locator), a network address, often made of memorable words, e.g. bklynlibrary.org. Each domain name is linked to an IP address.

Domain Name Server (DNS), the phone book of the internet. Domain Name Servers contain a directory of domain names and IP addresses that these names are associated with.

Email Host or Provider, an organization that operates email servers, e.g. Gmail (Google), Yahoo, Riseup.

Email Server, a server that handles and delivers email over a network such as the internet. Mail servers can receive emails from computers and deliver them to other mail servers.

Encryption, the process of encoding a message or information so that only authorized parties can access it. Encryption can refer to data at rest (data that is encoded when it is not moving through networks) and data in transit (data that is encoded while it is flowing through a network).

Things that can be encrypted include Email, SMS/texts, Documents, Messaging (Signal, WhatsApp), Video...

Encryption Protocol, a method used to encrypt data. There are many encryption protocols, some that work for specific types of communication like web browsing (HTTPS, TLS, SSL), email and documents (PGP).

End to End Encryption, a system of encryption where only the writer and the recipients of a message are able to read the message.

Full Disk Encryption (FDE), is a term that means that everything on a disk from data to software to an operating system may be encrypted.

Hardware Token, a hardware device used in 2-Step Verification/2-Factor Authentication processes to authorize use of a service. Commonly, these are in the form of a smart card or a key fob.

HTTPS, also called HTTP over TLS, HTTP over SSL and HTTP Secure, encrypts data flows on a network. When you see this "S" in the browser's address bar, the information you send to and receive from the site is sent encrypted, so that a person watching the traffic on your network will not see the full content of what you are communicating.

Internet Browser, software that communicates and presents data on the internet, e.g. Safari, Firefox, Chrome, Internet Explorer.

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

Internet Protocol Address (IP), a unique address assigned to each device on a network that works like a return address on a piece of mail. If you send out a data request from a computer, the computer marks or identifies your request with your IP address, and the results will be delivered back to the device on that IP address. In a network, some devices may have static (constant) or dynamic IP addresses assigned to them. An IP address consists of a series of numbers, like 172.16.254.1 or 2001:db8:0:1234:0:567:8:1. Some of the segments of numbers indicate the network you are on, and some indicate the device you are on.

Internet Router, a device that connects networks. Routers connect networks to one another on the internet and have the critical job of keeping data flowing as efficiently as possible from one network to another.

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

Mass Surveillance, a method under which large numbers of people have their communications, whereabouts and/or activities recorded. May be neutral, but can be used for nefarious purposes.

National Gateway, a router that serves as an entrypoint for the internet in your country. Internet traffic to and from any device passes through the national gateway as it is being routed to your device from the internet. Therefore, in the national gateway is also a place at which internet traffic can be monitored.

Organizational Security Policies, internal policy whereby an organization has plans in place to pre-emptively and otherwise address digital and physical security

Password Managers, cloud-based or local software that stores passwords to multiple accounts, usually with one key password to unlock the software.

Personal Data, information that can be used to identify an individual person, e.g. birthdate, name, social security number, address.

Phishing, email fraud method that attempts to gather personal and financial data from the recipients, e.g. a deceptive request for money in times of need that appears to be from someone you know, or a link to a fake financial website in a message.

PRISM, a code name for a program under which the United States National Security Agency (NSA) collects internet communications from various U.S. internet companies.

Private Browsing, also called privacy mode or incognito mode, is a feature of some web browsers that often includes the ability to disable the retention of browser history, caching, and cookies. This setting does not impact the information that is transmitted or sent through a network.

Risk assessment, a process to identify and evaluate the likelihood and impact of risks, in this case, related to digital data and communication. This process supports an organization in prioritizing concerns and considering possible threats.

Server Farm, a cluster of servers, ranging up to thousands of servers.

SMS (short message service or text messaging), commonly referred to as a "text message" by which you can send a message of 160 characters between mobile phones and PCs

Software Token, a piece of software used in 2-Step Verification/2-Factor Authentication processes to authorize use of a service. Usually, a software token generates a code for a user to enter to authorize their access.

Spam, irrelevant or inappropriate messages sent to a large number of recipients.

Third Party Service, a service that is provided by an entity other than the users (i.e. staff, patron) and the service they are directly interacting with (i.e. the library), e.g. BiblioCommons.

Tor Network, is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. It bounces communications around a distributed network of relays, prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Updates (to a Software and Operating System), sometimes called a software patch, is a free download for an application,

operating system, or software suite that provides fixes for features that aren't working as intended or adds minor software enhancements and compatibility.

Verification, or authentication; proving that the person logging in is who they should be.

Verifying off-band, checking in another modality, such as in person or through text message to make sure the correspondence is legitimate.

Virtual Private Network or VPN, is a service that lets you create a connection to another network over the internet—ideally, a secure and encrypted connection. The easiest analogy to describe a VPN is as a "tunnel"--you connect at one end, your requests are handled at the other end, but the traffic in between is encrypted and therefore not visible to intermediaries

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

Web Cache, temporary stored web documents such as HTML pages and images. Caching reduces bandwidth use and load time when a web page is visited.

Web Host, an organization that provides services for maintaining a website, including web servers. Some web hosts also provide domain name registration and email service.

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

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.

Thanks to the Data Privacy Project (dataprivacyproject.org) for some of the terms and definitions.

Stronger NYC Communities Organizational Digital Security Guide

Build Power - not Paranoia!

Visit: https://strongercommunities.info