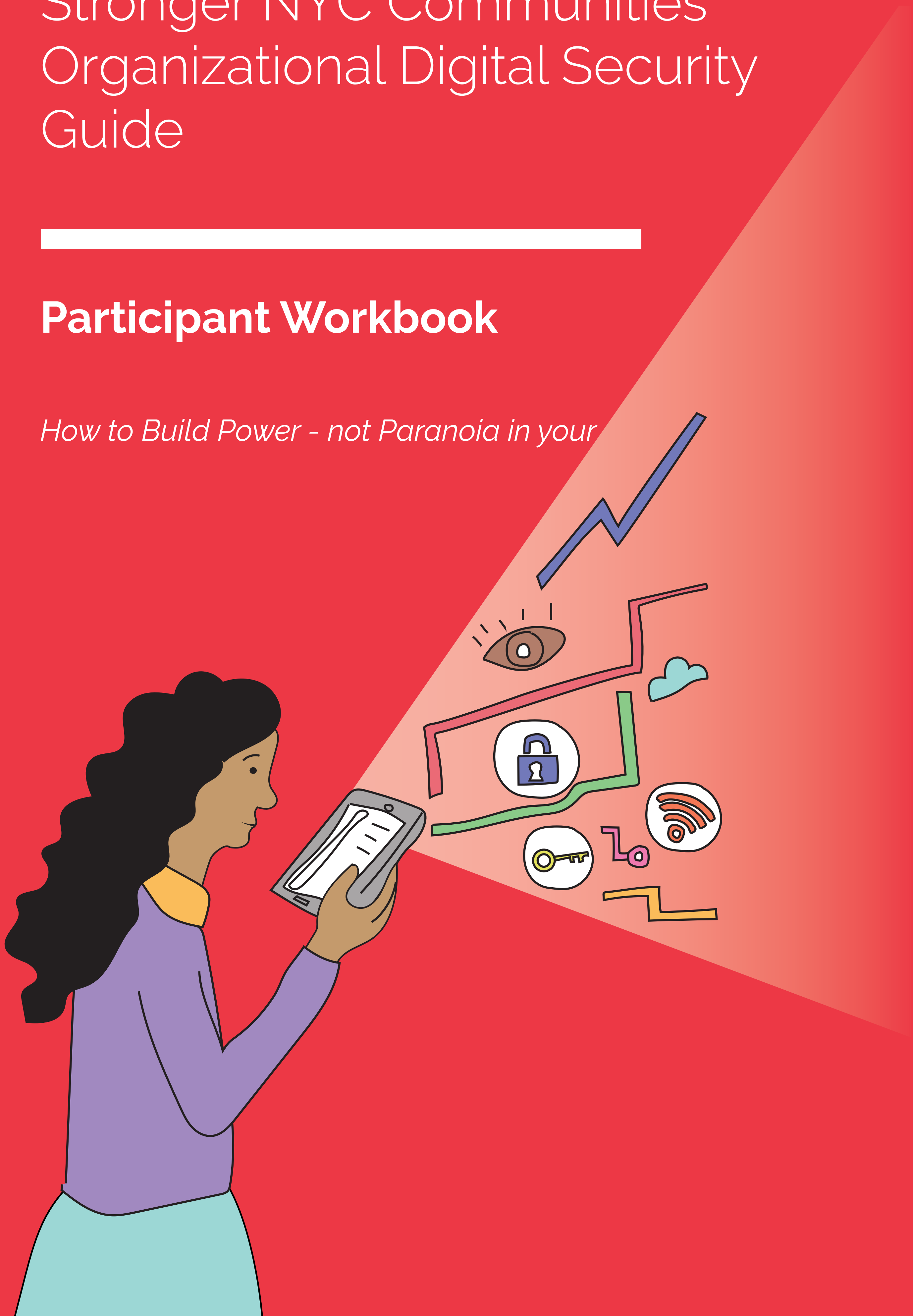
Stronger NYC Communities Organizational Digital Security Guide

Participant Workbook

How to Build Power - not Paranoia in your



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 PARTICIPANT WORKBOOK

This guide provides ideas to help organizational digital security workshop participants learn and do the work, homework and handouts, and a readings and resources list.

03

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?

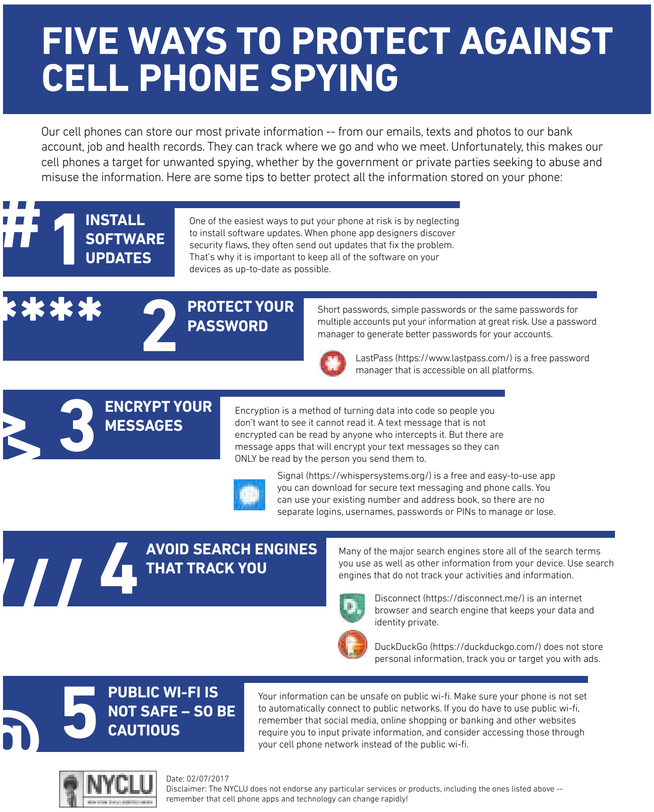
Begin to draft a checklist of 'services this employee can access,' and how soon they can access them (1 week, 3 months, immediately, never without supervision, etc).

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.

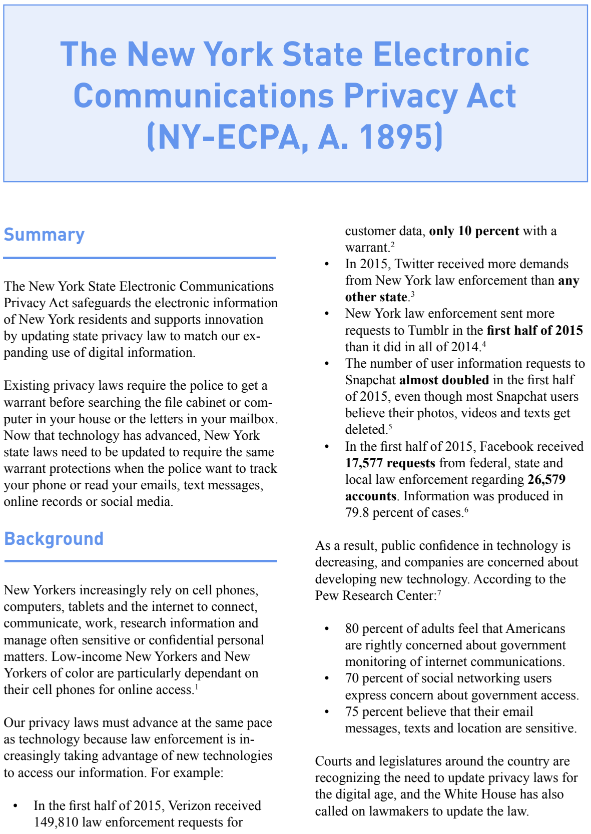
DuckDuckGo (https://duckduckgo.com/) does not store personal information, track you or target you with ads.

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.

Stronger NYC Communities Organizational Digital Security Guide

Build Power - not Paranoia!

Visit: https://strongercommunities.info