Stronger NYC Communities Organizational Digital Security Guide

Resources

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

04

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

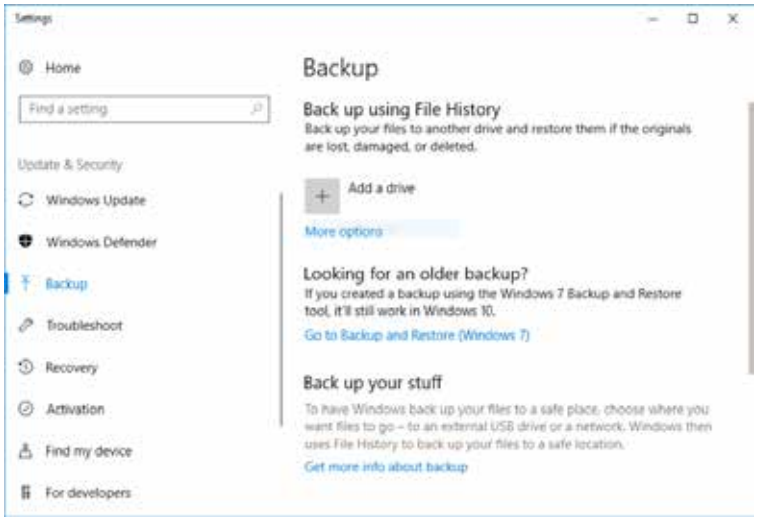
Safer Backups

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.

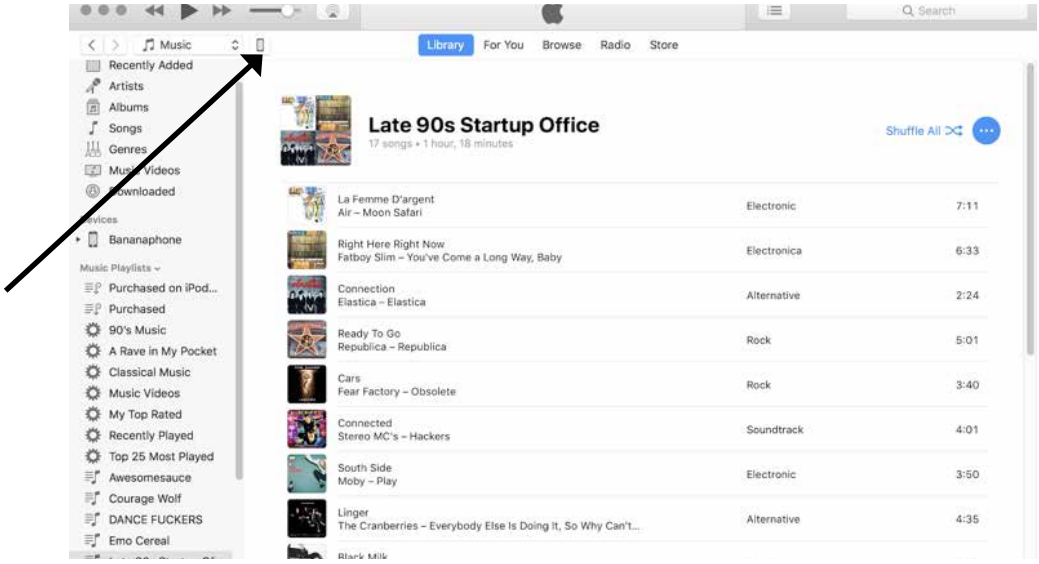
NOTE: Windows does not encrypt the drive automatically. For encrypted backups on Windows, you can use a paid end-to-end encrypted backup service such as Spider Oak's Backup One (https://spideroak.com/one/).

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

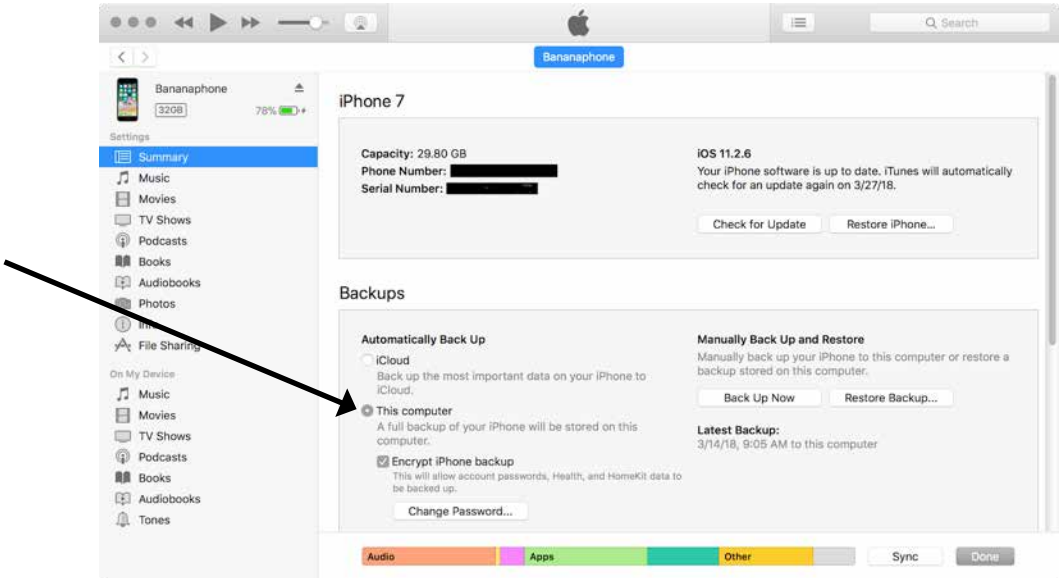


Backups - in Mac & iOS

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 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