Prepared by Brandon Smith for Northwestern Medill SJNN. Feb 2019. Reviewed for accuracy by (and including suggestions from) Micah Lee of The Intercept.

Security isn't a set of tools; security is a mindset.

- You'll often encounter a situation that doesn't fit the mold of what you're learning here, so you need a mindset to figure out how to deal with the situation. A mindset will allow you to extrapolate from what you know and figure out ways to deal with unfamiliar situations.
- Sometimes the mindset of working in a secure way is called "operational security," or "Opsec," as it's abbreviated by national security workers and other folks who get nerdy about it.
- To me it means, basically, don't be lazy. Learn all you can about what capabilities your potential threats have, and keep abreast of the latest news on it. And don't be afraid to make other people think you're going too far, or being too "paranoid." This isn't you you're being paranoid for you; this is mostly for your sources. We'll get into making promises to sources later, but suffice it to say that you don't want to be known as someone who broke or couldn't fulfill a promise for a source who counted on you.
- Security professionals think in terms of an "adversary"—who you're most likely to have to defend against to get the job done right. If your adversary is a member of, say, a county commission of a low-population county, you might have a lot less to worry about than if you're working on a story with national security implications and your adversary is the full weight of the U.S. government.
    - But beware with this calculation, because many cities, Chicago included, have connections at the city level (via the police) to a federal "fusion center." These were formed after 9/11 to share intelligence, theoretically for good reason. (9/11 may have been prevented with better intelligence-sharing.) Now they serve as ways for the feds to pay for surveillance equipment that cities and counties then use. Often they then share the procured intelligence with the feds. (Federal law about surveillance on citizens is sometimes more restrictive than local law, so in this way, the feds can get around their own limitations.)
- So fusion centers are a way for feds to get local authorities to do their dirty work... but it's also a way local agencies can use some of the feds' capabilties to their advantage. So don't think that if you're dealing with "just" a city office, you won't occasionally face nation state-level technology/capabilities. There won't be the same sophistication as on on a three-letter agency's "targeted" effort, but it's not just Mayberry anymore in cities.
- *From Micah Lee: "Threats can be very diverse, too. Maybe you need to worry about your source losing their job; getting deported if you're dealing with immigration stuff; or even physical violence, depending on the type of story. I can see #metoo type stories where sources are in real danger but from very low-tech and personal surveillance."* On these, often gendered, situations of threats of violence (which includes de-anonymizing someone), a source crashing at another person's house while everything goes down might be an easy fix.

Why it's not paranoid to go to great lengths to protect sensitive sources

- Here's an excerpt of the top of just the latest journalist-spying story, published by Reuters on January 30 with the subheadline "Ex-NSA operatives reveal how they helped spy on targets for the Arab monarchy — dissidents, rival leaders and journalists.":

  > Two weeks after leaving her position as an intelligence analyst for the U.S. National Security Agency in 2014, Lori Stroud was in the Middle East working as a hacker for an Arab monarchy.
  >
  > She had joined Project Raven, a clandestine team that included more than a dozen former U.S. intelligence operatives recruited to help the United Arab Emirates engage in surveillance of other governments, militants and human rights activists critical of the monarchy.
  >
  > Stroud and her team, working from a converted mansion in Abu Dhabi known internally as "the Villa," would use methods learned from a decade in the U.S intelligence community to help the UAE hack into the phones and computers of its enemies.
  >
  > Stroud had been recruited by a Maryland cybersecurity contractor to help the Emiratis launch hacking operations, and for three years, she thrived in the job. But in 2016, the Emiratis moved Project Raven to a UAE cybersecurity firm named DarkMatter. Before long, Stroud and other Americans involved in the effort say they saw the mission cross a red line: targeting fellow Americans for surveillance.
  >
  > "I am working for a foreign intelligence agency who is targeting U.S. persons," she told Reuters. "I am officially the bad kind of spy."

- It may be a 1% chance that someone is looking into you, but even that is unacceptable and warrants 5x or 10x extra work. (Often it's just 5-10 seconds for a password type or secure app opening, versus 1-2 seconds otherwise.) Particularly when the consequences are your source—who's helping you and helping the public—potentially losing their job, future career prospects, or, heaven forbid, their freedom.
- Your story may not seem important to you; it's not gonna get anybody killed, imprisoned, or even fired. So is this worth it? Maybe on a feature story about a new restaurant, no. Or if you're regurgitating a press release. But if you're doing the kind of work that matters, the kind of work that tries to right a wrong, then someone will have been doing the wrong. Someone stands to lose some professional ground. Presumably someone with some power. And people can get crazy with their reputations.
- Don't take your sources' risk lightly. If found to be a leaker and they lose their job, it may not be just that job they've lost. They may become persona non grata in their entire industry. And if they've trained their whole lives for that career path, it can be exceedingly hard to "pivot" to a different industry.
- The Intercept was founded on source security, but they've had a couple high-profile cases where it seemed like they had mis-steps:
  1. The presumed FBI agent whistleblower who likely gave TI documents showing a myriad of the FBI's internal rules
  2. Reality Winner, who has said she divulged a seeming large part of what the intelligence community knew at the time about Russian hacking (that is, disruption of all kinds) of the 2016 federal elections
- Here's what Micah Lee (of TI) says about those cases: *"Sadly in both the Terry Albury and Reality Winner cases, I think there was little we could have done to prevent them*

from getting caught. In Reality's case there's a lot we should have done better, but even if we did it all perfectly, she almost certainly would still have gotten caught because of how things happened on her end that were outside of our control. In fact the affidavit against her doesn't mention printer dots or anything like that. She was one of the like 6 or 7 people who accessed that document, and of those people she was the only one who had any interaction with the Intercept – she once wrote an email asking for a transcript of Intercepted (TI's podcast). That alone made her the prime suspect. And the Intercept didn't know any of this – we just got a document in the mail. (And from that alone they had to decide whether to publish it, which they did.) This is something I've learned doing security at the Intercept for years, that so much of protecting sources is out of our control, even if we do everything right. But all that said, keeping an opsec mindset is absolutely critical for protecting sources when it is in your control."

  - This might be a lesson to all of us to try to write good instructions on your blog's or news organization's webpage for whistleblowers. Those should include statements about not interacting with you (or your organization) in trace-able ways prior to a whistleblowing situation. And if they've done that already and still feel led to blow the whistle, try to work with them to broaden the universe of people who had access to the information you're publishing about. (Which probably means de-specifying the actual information you're publishing.) Maybe include this kind of knowledge in your public webpage. That it behooves them to enter into a conversation instead of just dropping documents, mostly for their own safety—so the outlet can de-specify the information enough that they have a fighting chance.

- Keep in mind that it can be cheap to hire someone to spy. Vice's Motherboard this year hired someone for $300 and they tracked the location of a hypothetical target from just a phone number. Somehow the person's mobile carrier was leaking, or selling, their location data. Possibly via SS7.
- The cell tower internet backbone, called SS7, is famously insecure, open to both governments and low-cost hackers in equal measure. It might be an extra step to get **content** of, say, text messages, but it's easy to get metadata: who you've been texting and precisely when. If you've made your cell number public, your adversary can buy leaky metadata from that and cross-reference it with numbers associated with their internal investigation. If your number isn't public, the investigator can get metadata from everyone who may have had contact with the information, and see whether any of them have tried to interact with anyone at your organization, or indeed, any reporters whatsoever.

Threat modeling and controlled access

- I mentioned brainstorming who your most-capable "adversary" is. Or if you have more than one adversary with different **kinds** of capabilities, you might need to consider them both. A "threat model" is basically an attempt at estimating the capabilities of that adversary so you can take appropriate measures to defend against them. What does it mean to "defend against" an adversary? Basically it means making the surveillance they'd need to meet their goal prohibitively expensive for them.
- One of the key questions you and your source(s) face is, as we mentioned above, how

many people have access to the information you both want to publish. If just three or four people have access, your source is kind of a sitting duck. That investigation will be very short, and they will end up facing the consequences of being discovered. Always be honest with sensitive sources. Tell them you plan to keep private that which they intend to be private, and only make public that which they intend to be public. (They should be in control of the information they're sharing that you wouldn't have had without them.) Make sure to tell them that, while you're endeavoring to keep certain things secret, you may fail; you may have estimated your threat model incorrectly.

  - Be upfront about the security training you've had. If it's just a day, that's not very much. No matter how good the teacher. If you're in a serious situation, best to call in big guns—people like Micah Lee, who do security for a living. (He specifically has been good about helping journalists in need, so try e-mailing him.) Of course I'm also available to consult.

- If I'm facing a situation where my source is one of three, or even seven, people with access, I'm going to try to obfuscate the actual data in my story. Not reporting on a situation as specifically as I can never feels great... but broadening that scope, pulling that camera back a little, may mean the difference between this person losing their livelihood and keeping it. You can use the specifics internally as a means of vetting the documents you've got... but for the public, it might have to be reported as something that a wider swath of workers had access to. I tend to shoot for 20+ workers, or even 30+, to make the investigation such a huge timesuck and money-suck that it will be impractical. Again, you'll have to ask your source whether they had any contact with you or your colleagues or organization (or even any journalist or news organization!) prior to the actual whistle-blowing.
  - Even just being known around the office as one of the more critical of the organization's mission (or it's means) can make investigators focus on them. I say this not to scare would-be whistleblowers away; rather to make you help them understand the risk—and for both of you to properly estimate the obfuscation you'll eventually have to do in whatever you publish.
- So the goal is to make a proper search impractical for your adversary. Impracticality, of course, is all based on how much resources (money and legal authority) your adversary has. If your adversary is Jeff Bezos, consider him on par with a nation-state and don't use any electronics. If it's Chicago's mayor or the C-suite of a Fortune 100 company, don't do anything over un-encrypted channels. If it's a school board of a small town, you can probably text in the clear with abandon... but not if your source is using a work-issued computer/phone, or work account, to contact you. I hope this goes without saying.
  - Remember the example where they've contacted you before their whistle-blowing? If they've done it from a personal account but using a work computer, they may be compromised or may not be—depending on how closely their employer monitors that computer. If they've done it from a work **account,** of course their cover is blown. If they're in the intelligence community, even personal accounts on personal **devices** may not be safe.

One unencrypted contact spoils the whole barrel

- I've had people reach out to me first via Twitter—an "at" mention, not a DM—and then that person was hoping to have a secure conversation. Well Pardner, too late. Even if you delete the tweet, there are likely some permanent logs. So what's the solution? Post your Signal number publicly, and encourage folks to reach out via Signal *FIRST* if they want to pass you something they think could be news. I post my standard cell number, but this tutorial (By Micah Lee!) shows how to make a new number for use with Signal that isn't your actual cell number.
- Again, if you're doing national security reporting or want to, think about posting a physical mailing address on your public profile, because Natsec professionals' devices can't be trusted to be free of government spyware. That said, beware that, especially if you've had one or more good natsec stories published, there's a chance you'll be watched by an agency in some measure. So even a mailing address you post could be subject to undetectable mail interception programs. Opening & re-sealing, or X-ray inspection. (This has been reported in well-vetted outlets.) The best solution for national security stories might be new post office boxes for every new story, whose addresses/numbers aren't published publicly. In that case, mention on your public profile that if they can use another method of contact to start, you can get therm a new, un-published post office box address for them to use with you.
- Alternatively for natsec reporting, you could use SecureDrop/OnionShare with new devices bought with cash for this purpose only. That's to get around the possibility of malware already installed on their (or your!) personal device(s).

Metadata in aggregate is content

- Metadata is just as valuable—if not more valuable to someone wanting to discover your sources—as the actual contents of your communications or notes. So what metadata are you giving off?
    - Your location, at all times. Everyone has a phone in their pocket. Because of how phones connect to towers, your carrier knows where you are at all times to a precision of something like 15-20 feet. This may not seem like a big deal but all carriers have a price for the location data they're selling (and they are selling it). That means that the collective network of data brokers—most corporate spying is done via shady "brokerage" firms—has everyone's location, both in real time and historically. It can be used to determine who you are in close proximity to on a regular basis, but also determine who you've met with, at least to a certain degree of probability. If a leak investigation has only five potential targets; no one's an office rabble-rouser; and there's no record of any of them reaching out to reporters... then if your adversary is sophisticated enough, or desparate enough, they could turn to a broker of location data to see if any of their investigation's subjects met with the reporter who wrote the story. (Three-letter agencies might have their own trove of historic location data, so they might not have to rely on private entities.)

        - What can your location data reveal about a person? You might be surprised to learn. In a 2014 US Supreme Court case that ultimately prohibited local police from putting GPS transponders on anyone’s car without a warrant, the successful side showed the court what just 30 days of location data can reveal about a person.

- Whether you have a pet and how well you treat it
- Whether and how often you visit each member of your family
- Whether you’re late to work frequently or do any non-work thing on work time
- Whether you’re faithful to your partner, and if unfaithful, with whom—and that person’s gender and other things about them
- Whether you’re seeing a medical professional and what speciality, including therapists
- Your religious affiliation
- Whether you frequent a bar or place of gambling
- Whether you exercise or smoke (which health insurers desparately want to know)
- Whether and how often you buy groceries and/or eat takeout
- Whether you’re involved in any legal matters

- You’re giving off other metadata than location, to the NSA and to SS7, which, again, is accessible by the inexpensive underbelly of brokers and mercenaries. That includes your metadata of texts and calls (unless you use Signal/WhatsApp). That’s who you called, when, and how long each call took. Maybe also the location that each call was made from.
- Email merits a mention because Micah suggests avoiding email altogether when dealing with sources who need security. Maybe because metadata that leaks from email includes dates and times, to/from lines, and ***subject lines***. In addition to the three-letter agencies, this can be intercepted by your ISP or carrier, and thus anyone who can buy or filch the data from them. If anyone wants to check out your email metadata, or that of your source, they’ll be able to do it historically.
  - There are ways to use email, such as creating ProtonMail accounts just for the purpose. But you have to be able to trust that there’s no workplace spyware or random malware on the machines. There are other things to watch for, so write Micah to ask, or just use Signal.
- Everything you post and people send to you on social media is “leaked,” but you already knew that. Still, you’d be amazed what we forget we post there. It’s sometimes worth a review of your own account, or your source’s account, to check. An investigator, if they’re desparate enough, will go back far into social history. Direct/private messages don’t have public metadata, but if a source DM’ed you from a work-issued device, you should assume that communication isn’t secure because you can’t trust how closely that device is monitored. (Not live, but rather recorded for historical analysis.) And if you’re working with a story with possible interest from law enforcement, the messenger (such as Twitter, Facebook, etc.) could get hit with a subpoena for that message record. You’d

never know of the subpoena...until your source is indicted. The adversary would likely subpoena the DM records for anyone in the universe of their investigation—anyone who had access to the info you published, minus those they've already ruled out. What kinds of published matreial is of interest to law enforcement? Anything in a situation where:

- The actual leak itself could be prosecuted, like information about national security
- The story topic is something that would want to be suppressed by law enforcement itself (Laquan, say)
- a city official who has influence over law enforcement (like the mayor's office);
- or even, possibly, someone to whom the mayor or police chief owes a favor. You never know. This is unlikely, but the question is: can you afford to risk what your source stands to lose?

Micah reminds us that security researchers have discovered Twitter keeps direct messages even after both parties have deleted the messages. That means they're subpoena-able forever. Link to story: https://techcrunch.com/2019/02/15/twitter-direct-messages/

Remember document & photo metadata

- Famously, a reporter from Vice outed the location of John McAfee, of antivirus fame, after granting him location anonymity for their interview because he was wanted on criminal charges as a suspect in his neighbor's murder. The reporter led investigators right to McAfee via not scrubbing the metadata of a photo.
- *Scrub metadata from photos using online tools. A tip from Micah if you're working quick-and-dirty: "Open the photo or document and take a screenshot of it – the screenshot could have its own metadata, but won't retain any metadata from the original document which is the important part"*
- Documents can have their own metadata. All printers and photocopiers apparently print invisible dots that serve as signatures that can often lead back to *individual machines*. It's uncanny. Just yesterday (early Feb 2019), Axios re-typed 95 pages of documents they got from their source in the White House. It's tedious but it's one way to be able to use facsimiles of the original docs without leading investigators to your sources.
- From Micah: *"In Terry Albury's case, the (FBI) used the fact that every odd page has a discoloration in the corner as evidence that he displayed the document in a 2-page layout on his computer and took photos of the screen, and there was a discoloration in the corner of his screen."*

Half of this job of keeping your research and your sources secure—or maybe more than half—is serving as a teacher to your sources.

- When they mess up on security, it's just as bad as when you mess up. One and the same, because the outcome is the same. And the world will blame you. But regardless of perceived blame, it makes little sense for you to implement a security protocol if your source isn't following the same protocol—or at least a similar one based on the same threat model.

- It behooves you to get good at teaching all of this stuff; to be a patient teacher; to know *why* you're asking them to do what you're asking them to do, so they also believe in the "mission" and take the medicine as prescribed, so to speak.
- From Micah: *"Sources often have their own biases and superstition about opsec, and sometimes you have to just work with them on it. Maybe their friend told them Telegram is the most secure and you can't trust Signal – so maybe you need to do some research on Telegram and figure out how to use it in as secure a manner as possible to help protect them."*

Remember Fusion centers? The sites of national/local intelligence sharing? It helps to know the capabilities of "Stingrays/Hailstorms"

- These $200,000 boxes produced by a single Florida company, Harris Corp, are in use by jurisdictions around the U.S. They pose as cell towers. It's a type of attack called a "man-in-the-middle," (I'm sure you get the analogy), copying and passing along everything as if they're not there, and you're none the wiser. End-to-end encryption defends against this because everything a MITM intercepts is scrambled.
- Sound like a civil liberties violation? Indeed. Stingrays and their sequel, the Hailstorm, use a loophole in a SCOTUS decision. That 2014 decision says we have a privacy interest in the data on our phones after we're arrested. (SCOTUS basically said that, after you're arrested, police can't copy your phone data.) Unfortunately, Stingrays/Hailstorms copy much of your data—that which goes over the air—prior to arrest. Lots of folks are waiting for SCOTUS to hear a case, any case, that challenges the loophole.

End-to-end encryption

- What we mean by "end-to-end" is that content, and hopefully some or all metadata, travels encrypted the entire distance between devices. It should be encrypted on your device before it leaves and only unencrypted once it arrives on the device of the person you're meaning for it to go to. *From Micah: "(The most common) end-to-end encryption doesn't help much against metadata. Like, iMessage and Facetime are e2e which is great, but Apple (and thus anyone who can subpoena or has backdoor access to Apple) can see 100% of the metadata."*
- Google will say Drive is "encrypted." It is but only for like 90% of the steps it travels between your computer and your recipient's. There's a part in the middle where Google itself sees the following in an unencrypted way:
  - metadata about how you use the products (ostensibly to refine the products themselves but they very well may sell this data about you and how you work), and
  - likely the content itself—to further profile you, which is their true business and indeed how they pay to host and maintain all this infrastructure).

  So do you need to take into account Google Drive's vulnerabilities in your threat model? Probably not. Unless your model includes as an adversary the full U.S. government; someone who can plant malware on your machine to see what ends up on your screen (or someone who can hire someone to do so); or Google itself! Maybe it goes without saying: if you're covering Google, don't use Google's tools to do it.

- Key example of end-to-end encryption is Signal. Mostly it's used for texting but if both folks have robust internet connections, you can do a video chat or audio call; crucially, also, Signal's desktop client is a good platform for file sharing. (Drag and drop!)
  - In a pinch, if you manage your own version control with your collaborator, like with numbered filenames corresponding to edits, Signal makes a great encrypted collaboration tool. (One hotly anticipated encrypted collaboration tool, Pursuance, is still in development. I've been a consultant to the developers.)
- In a pinch, if Signal isn't an option for some reason, Jitsi probably works for encrypted video chat. It's browser-based—no download required—and easy to use for first-timers. *From Micah:"You still have to pick a Jitsi Meet server you trust, because a malicious server can in fact spy on the video calls. (Jitsi) is a better option than big centralized video services like Google Meet/Hangouts or Skype, because it's an open source project and you can use a service you run yourself or by an org you trust. Most people just use meet.jit.si, and I actually wonder how much of a target that server is for hackers."*
- Don't bother with PGP unless you're an expert and your source is, too. It's too hard to keep your private key secure, and your historic messages are in danger in the event your private key is compromised. This is possible if your device is ever "pwned," AKA, surreptitiously in the control of a malicious actor via hacking or malware. They'll be able to decrypt everything you've ever sent with the key they now possess. With Signal, the most they could get is two messages, because the key renews every other message.
- On stories where the threat model is a powerful actor, or you know the actor has some serious computer skill in their arsenal, consider the fort knox of secure communications: the SecureDrop system... or if you don't have access to an outlet with a functioning SecureDrop, Onionshare seems a nearly equally-good option. (Also a Micah Lee development project!) I won't go into them in depth here because there's plenty of documentation on them online as to how they work and what they don't protect against.

Caveats

- If your source's device is already pwned by the adversary, no encryption tool will work. Luckily, targeted surveillance can be very expensive, and thus it can be assumed to be relatively rare on personal devices. (Company spyware on work devices is common.) The chances go way up as you involve topics and/or personnel re: national security, and companies with huge budgets and lots to lose from your exposing their practices.
  - Encryption keys for end-to-end systems like Signal necessarily "live," or reside, on the devices—so if someone has complete access to the device, whether physically or remotely, all bets are off and you have to flash/restore the device... or in some cases, just get a new device or use fully analog means of communication.
  - That's what a big "blockbuster" NY Times story on Signal supposedly revealed. But if you know how this all works—and if you're reading this, you do now—you know encryption work. That is, barring company spyware or malware from a

campaign of targeted surveillance.

- Contemplate the possibility that YOUR device may have been pwned.
    - How do you defend against this? A few ways. Install software updates as soon as you possibly can after you're told they're recommended or available for you. OS updates, app updates on your devices. Many (if not most) of these updates are fixes to security holes someone discovered.
    - Defend against fake links, the main method of phishing. Check URLs of links sent to you by hovering over them before you click on them—and keep familiar with the actual domains of the sites you use.
    - From Micah: *"Also, use disappearing messages as much as you can! If you've talked to your source for a year before one of your devices gets hacked, or confiscated and searched, you don't want that years' worth of messages on it"*

Kinds of security other than communications

- Online hackers looking to steal identities — rainbow tables and passwords
    - If you want to learn why YOU NEED A PASSWORD MANAGER, read this cool Ars Technica article. Ancient history from 2012, but it's still applicable today, and even more so as techniques and password database leaks have advanced.
    - Make at least 3 dice-based passwords to unlock:
        - the password manager
        - your device screens (computer and phone; use 3 words for the phone)
        - any external/backup/flash drives with story info on them
    - Use EFF's word lists to make dice-based passwords
- Data at rest — properly storing your research
    - Do full-disk encryption on your device. Often it's something you have to go to your settings to do, so look up your device, and how to do full-disk encryption on it, via your favorite search engine.
    - FULL DISK ENCRYPTION MAY NOT WORK IF YOU DON'T FULLY SHUT DOWN THE DEVICE. Most of us just sleep our phones and computers. THAT'S WHY YOU NEED A STRONG SCREEN LOCK PASSWORD.
        - Apple screen locks are strong, and I'm using that in a technical sense. It's basically encryption. But if you're not using an Apple device, you should research whether the screen lock on your device can be brute-force opened and your devices' content downloaded. If not, you may need to shut down your device whenever you're not physically with it (or if you're going into a dangerous situation), to activate the disk encryption.
        - Fingerprint unlocks were, for several years, able to be compelled by law enforcement. As such, security-minded folks were advocating for journalists to not use your fingerprint for screen-unlocking purposes. While that has changed as of a late 2018 federal court ruling—you now cannot be compelled to unlock your device with your fingerprint—I still don't use a fingerprint unlock. That's in case some po-dunk law enforcement agency didn't get the memo from this federal court. Also, better safe than sorry in a situation where you're more likely to be

searched, like a border crossing or protest. You never know what legal BS they'll pull to do what they want to do.

- Browsing
    - Can you think of any party—any party at all—that you wouldn't want knowing what you're seeing or searching for online? Then you might want to protect your browsing.
        - Tor is the gold standard but can be slow. Isn't necessarily prohibitively slow. Try it.
        - VPNs are good and can help you use the Internet in various ways ("the Internet" is more than browsing, whodathunk!) but you pay for them, usually monthly. The site Boingboing sometimes has deals for lifetime subscriptions to VPNs that seem to have decent privacy promises (re the logs they keep). But *any* VPN business is gonna give you up to law enforcement to save their business if it comes to that. (Talking about National Security Letters, subpoenas, other dark arts.) So get as good a guarantee as you can... and from there just realize that using the internet through a VPN isn't a guarantee of security for all time. Unlike with end-to-end encryption, you don't have all the power here. VPNs are also good for some semblance of security on coffee shop wifi networks. (See below.)
        - *From Micah: "Think about your browser history. Maybe delete it regularly or use a browser that lets you not even retain it at all (Chrome doesn't let you do this, Firefox does, and I think maybe Brave). Understand what private browsing mode/incognito mode protects against and doesn't protect against, and actually use it when you need to do internet research that doesn't log your history.*
        - For the record: Private mode/incognito mode doesn't do anything except prevent you, or anyone who accesses your account on your machine, from seeing browsing history. It is by no means an encryption tool for what travels over the wires.
- Wifi connections
    - Maybe you don't have sensitive data on your machine now... but if you ever want the opportunity to do so in the future, you should try starting now to avoid malware. 'Cause it might remain on your machine until it counts. A good start to avoiding it: try to avoid "open" wifi networks, which you can use without any credentials, or with a single credential the whole coffee shop is using. Probably you'll have to rely on them in a pinch. But limit the number of times, and number of minutes, that you do, and you'll minimize your exposure.
    - Try to only use networks where you're given a username and password unique to you. Like your school's network. Then, at least, a malicious actor would need to use social engineering against that system to gain their own login credential. It can be done but skyrockets the cost of the operation beyond what most adversaries are willing to pay. (And some advanced networks, like at some co-working spaces, provide entirely separate (virtual) networks for each user

credential. These are virtually un-hackable.)

- Coffee shops that just have you give your email address (or nothing at all except clicking through a terms-of-service document) aren't ideal, either. *From Micah:"If you do want to use public networks, make sure to always connect to a VPN immediately after clicking through the captive portal. This will prevent attacks on the same network, including randos at the same coffee shop that know how to use Wireshark, from monitoring your internet."*