Digital security and privacy workshop – Intro segment

Jul 03, 2018

Contents

This workshop is designed to be read collaboratively/collectively, going around in a circle. The text is based on

material from EFF and Equality Labs.[2]

[2] Sources:

- https://sec.eff.org/articles/harm-reduction
- https://sec.eff.org/articles/why-your-audience-should-care
- https://ssd.eff.org/en/module/seven-steps-digital-security
- https://sec.eff.org/articles/minimum-viable-teaching
- https://medium.com/@EqualityLabs/anti-doxing-guide-for-activists-facing-attacks-from-the-alt-right-ec6c290f543c

1 The Harm Reduction Approach

Harm reduction is a term used in public health to describe policies aimed at reducing the harm associated with high-risk behaviors, such as intravenous drug use. In the context of digital security training, the harm reduction approach can be applied to people that are at heightened risk of compromise because of their practices, such as using non-optimal hardware, applications, or platforms. It is not always possible to change somebody's (or our own) risky practices and when that is the case, it is important to meet people where they are, rather than where we think they should be.

Some principles to follow are:

- Everyone deserves digital security and privacy.
- Remove the stigma of bad security or privacy practices.
- Increasing your digital safety is a process.
- Harm reduction is collective.

1.1 Everyone deserves digital security and privacy.

It is not uncommon to hear people in the security industry say that if you don't use a certain product or you don't follow a certain best practice, then "you don't deserve security." This is a highly toxic mentality that causes a lot of harm. A techie may believe that activists should not use Facebook, but if activists still use the platform because it is a highly effective way of reaching their audience, then they need and deserve advice that allows them to be as safe on Facebook as possible.

1.2 Remove the stigma of bad security or privacy practices.

Everyone has made digital privacy or security mistakes, including trainers and "experts". Stigmatizing or shaming people for confessing their mistakes makes it less likely that other people will speak up about their own practices. Talking about our own digital security shortcomings is sometimes a good ice-breaker and helps make everyone feel more comfortable.

1.3 Increasing your digital safety is a process.

When learning about what we need to do to improve our digital security and privacy, it's common to feel overwhelmed. Don't be too hard on yourself – instead, we can see our work towards better security habits as a process that will take time. The goal isn't to lock everything down in one day or one week. It takes time and patience to learn, and it's important to give ourselves credit for how we have *already* improved our digital safety, even as we take further steps and solidify better habits.

1.4 Harm reduction is collective.

Because of the many ways our digital lives are inherently intertwined, it's important to remember that we are responsible for each others' safety and privacy. It's upon us to collectively support each other as we learn about each other's privacy preferences.

We can coordinate in reducing threats and vulnerabilities that affect us as co-workers, family members, activists, or even just neighbors using the same cafe WiFi to browse the web. When you notice that others have unsafe settings or are leaking personal data, you can tell them. If you prefer not to be tagged in photos on social media, let others know and ask others what their preferences are. If you see your parents have a weak password, take the time to explain how to create a more robust one.

There's a million ways we can help our networks reduce the harm from poor digital security habits and build better security cultures.

While many people often use military or war analogies when talking about digital security, thinking about it that way can often be misleading. In many ways, analogies to public health and medicine can be much more informative and helpful.

2 Why We Should Care – And Act

It's important to understand not just the what and the how of digital security, but the *why*. Why should we care about digital security? And, why should we take action to develop our personal security?

General tips and tricks about technology are great, but we also need to understand ourselves. There are several types of common thought patterns that can keep us from learning:

Nothing-to-Hide Apathy "I have nothing to hide, so why do I need to protect privacy?"

Security Paralysis "I am worried about my digital security to the point of being overwhelmed. I don't know where to start."

Technical Confusion "I'm ready to take action, but not until I have a perfect handle on how all of these technical concepts fit together."

Security Nihilism "There's no such thing as perfect security, so why even bother? If someone wants to hack me, they'll figure out a way to do it."

- What made you come today?

Genuineness and empathy is important. No one is perfect.

Many security trainers like to make their stories sound scary or intimidating. But these types of stories often turn people off from learning about security. Fear is the motivation killer, and can lead to "security paralysis" or other kinds of disengagement from learning.

Also, a single person can cycle through several of the attitudes below (and more!). The better we are at spotting and responding to our motivational hangups, the better we can learn.

2.1 Nothing-to-Hide Apathy

"I have nothing to hide, so why do I need to protect privacy?"

People with this attitude typically do not feel a personal stake in their digital privacy and security, and therefore do not feel compelled to act. They may associate digital security concepts with high-profile state actors, whistleblowers, and public figures – not with "normal" people like us.

Talking through the first step of threat modeling – the question "What do you want to protect?" can also be helpful towards finding your own stake in digital security.

Some examples:

- Credit card and bank account information (both on the associated websites and on any commerce websites like Amazon, PayPal, or Venmo).
- The information often found on "people finder" sites – like full names, home addresses, and family connections.

It's also common for the "nothing to hide argument" to become so dominant that we forget what's at play when we talk about privacy. What is privacy and what does it mean to people? What are we really talking about when we talk about privacy? This is a complex topic, but as one researcher puts it:

> Privacy is Consent. Privacy is the right to consent. Privacy is the right to withdraw consent. Privacy is nothing more than that, but that is everything.

Finally, sometimes someone with this attitude is making a logical decision based on their own threat model. Having identified what they want to protect, who may come after it, and what their risk is, they may have simply decided that a certain privacy protection is not worth them expending significant time, resources, or energy. The job of a trainer is not to "convince" them that they "should" take certain actions, but to help them make an informed decision.

2.2 Security Paralysis

"I am worried about my digital security to the point of being overwhelmed. I don't know where to start."

This kind of person cares deeply about digital security, but is frightened and paralyzed. Often, people with this attitude are overwhelmed with the task of locking down their personal information. Perhaps they have been bombarded with news stories about leaks and data breaches, or have close friends who have experienced personal harassment or doxxing. They may have even been exposed to intimidation-based trainings in the past that left them feeling overwhelmed and helpless in the face of various digital threats.

In this case, it can be helpful to emphasize one's personal agency. At the same time, acknowledge the reality that it may very well be impossible to control all the information about one person online – and *that's okay*. Instead, we can shift the goal from erasing all our information to just minimizing our information.

First steps to take could include Googling oneself (perhaps with the support of a trusted friend to help alleviate any fear associated with doing so), investigating social media settings, or looking into opt-out options on people finder sites.

The goal is to get the best idea possible of the information available about ourselves online, and then reduce it according to what we care about and are worried about. If we can minimize the information that we have control over, then we are in a much more powerful position if and when a company we use has a data breach or a social media platform we're on changes its default settings.

2.3 Technical Confusion

"I'm ready to take action, but not until I have a perfect handle on how all of these technical concepts fit together."

This kind of person may be technically overwhelmed. They are hearing about different kinds of devices, operating systems, apps, software, browser extensions, and encryption. While they have abundant information, they have no idea where to start or exactly how all these things are connected. Often, these learners have less experience with technology than the average trainer, but they are detail-oriented and cautious. They may be elders, or come from a low-resource background that has not given them consistent access to cutting-edge devices and software. Just like security paralysis, this person typically does not know where to start.

If this is your case, it can help to focus on the security principles behind the technology. Technology changes quickly and can be confusing, but fundamental security principles – threat modeling/risk assessment, tradeoffs, and deciding who and what to trust – can all act as steadfast guides as technology changes and evolves.

Security is more than just tools. It's about adopting a "security mindset" over time.

2.4 Security Nihilism

"There's no such thing as perfect security, so why even bother? If someone wants to hack me, they'll figure out a way to do it."

People with this attitude care about security, but also don't know what to actually do. Or, perhaps more accurately, they do not think they have the power to do much.

One useful concept is "**door lock security**." Think about the lock on the door of your home. It might be a normal deadbolt with a doorknob lock. This lock can be compromised in any number of ways: keys can be stolen or forged, locks can be picked, doors can be kicked down. If someone was determined to breach that door, they probably could. But you probably still locks your door regularly and finds some assurance in that level of security.

This analogy can even extend to extra layers of security. Perhaps you can imagine someone with particularly expensive items in their home having a security system protecting the perimeter of their house. Or, maybe they'd have a safe inside the house for valuables and important documents.

We can approach digital security in the same way. The digital security equivalent of a "door lock" can be reliable, reasonable, and worth using, even if it is imperfect and incomplete. For higher-value assets, added layers of security (analogous to safes or home security systems) can also be put in place.

The goal is to make it *harder* or *more inconvenient* or *more expensive* to hack you, not to make it impossible. It's important to set reasonable, achievable goals, not pie-in-the-sky theoretical scenarios.

3 Seven Keys To Digital Security

Here are some basic tips to consider when thinking about your own digital security.

1. Knowledge is Power
2. The Weakest Link
3. Simpler is Safer and Easier
4. More Expensive Doesn't Mean More Secure
5. It's Okay To Trust *Someone* (But Always Know Who You're Trusting)
6. There is No Perfect Security – There's Always a Trade-Off
7. What's Secure Today May Not Be Secure Tomorrow

3.1 Knowledge is Power

Good security decisions can't be made without good information. Your security tradeoffs are only as good as the information you have about the value of your assets, the severity of the threats from different adversaries to those assets, and the risk of those attacks actually happening. This guide should help you gain the knowledge you need to identify the threats to your computer and communications security, and judge the risk against possible security measures. And some of this knowledge you already have: knowledge of your own situation, who might want to target you, and what resources they have. You already have more power than you think!

3.2 The Weakest Link

Think about assets as components of the system in which they are used. The security of the asset depends on the strength of all the components in the system. The old adage that "a chain is only as strong as its weakest link" applies to security too: The system as a whole is only as strong as the weakest component. For example, the best door lock is of no use if you have weak window latches. Encrypting your email so it won't get intercepted in transit won't protect the confidentiality of that email if you store an unencrypted copy on your laptop and your laptop is stolen. That doesn't mean you have to do everything simultaneously, but it does mean that, over time, you should spend time thinking about each part of your information and computer use.

3.3 Simpler is Safer and Easier

It is generally most cost-effective and most important to protect the weakest component of the system in which an asset is used. Since having a simple system makes it much easier to identify and understand the weak components, you should strive to reduce the number and complexity of components in your information systems. A small number of components will also serve to reduce the number of interactions between components, which is another source of complexity, cost, and risk. That also means that the safest solution may be the least technical solution. Computers may be great for many things, but sometimes the security issues of a simple pen and notepaper can be easier to understand, and therefore easier to manage.

3.4 More Expensive Doesn't Mean More Secure

Don't assume that the most expensive security solution is the best; especially if it takes away resources needed elsewhere. Low-cost measures like shredding trash before leaving it on the curb can give you lots of bang for your security buck.

3.5 It's Okay To Trust *Someone* (But Always Know Who You're Trusting)

Computer security advice can end up sounding like you should trust absolutely no one but yourself. In the real world, you almost certainly trust plenty of people with at least *some* of your information, from your close family or companion to your doctor or lawyer. What's tricky in the digital space is understanding who you are trusting, and with what. You might deposit a list of passwords with your lawyers: but you should think about what power that might give them – or how easily they might be maliciously attacked. You might write documents in a cloud service like Dropbox or Microsoft OneDrive that are only for you: but you're also letting Dropbox and Microsoft access them, too. Online or offline, the fewer people you share a secret with, the better chance you have of keeping it secret.

3.6 There is No Perfect Security – There's Always a Trade-Off

Set security policies that are reasonable for your lifestyle, for the risks you face, and for the implementation steps you and your colleagues will take. A perfect security policy on paper won't work if it's too difficult to follow day-to-day.

3.7 What's Secure Today May Not Be Secure Tomorrow

It is also crucially important to continually re-evaluate your security practices. Just because they were secure last year or last week doesn't mean they're still secure! Keep checking sites like SSD (EFF's Surveillance Self-Defense guide)[1] because they will update their advice to reflect changes in their understanding and the realities of digital security. Security is never a one-off act: it's a process.

4 Some actual tech advice: The Minimum Viable Teaching

(When Teachers Have No Time To Teach or Learners Have No Time to Listen)

Sometimes there's no time for a full digital security walk-through. Perhaps you're suddenly about to face an unexpected set of risks. Too much information can be overwhelming or intimidating. You're short on time. You might have only one brief moment for security, and you want to take full advantage of it.

[1] https://ssd.eff.org/

Some security is always better than no security. You can do a lot to improve your basic security by walking through some basic steps, and following some general advice.

Here's a short bit of advice that can fit in one minute or less. It's a concentrated form of advice. This information could easily expand it into a half-day of teaching, but the short version is good too.

> "You can turn on encryption on your Android, iPhone, iPad or Mac. Pick a long password made up of six or more random words to lock your computer, or six or more numbers as a PIN to lock your phone. Don't reuse passwords! Use a password manager, or write down your passwords on paper and store it in your wallet instead. Turn on "two-factor" or "two-step" authentication on your Google, Facebook or other online accounts: this will help stop those logins from being hacked. Avoid clicking on strange links or email attachments. To send messages safely and securely, use an end-to-end encrypted messenger app like Signal or WhatsApp. If you want to be anonymous online, try using the Tor Browser."

Well, that was the concentrated version. Now let's break it down and talk about it.

The basics:

- Turn on encryption.
- Pick a long password.
- Don't reuse your passwords!
- Turn on two-factor authentication.
- Avoid clicking on strange links or email attachments.
- Use an end-to-end encrypted messenger app like Signal or WhatsApp.
- To be anonymous online, use the Tor Browser.

Here's some more detailed thinking about each of those pieces of advice, and how you might dig deeper into them, when you have more time.

4.1 Turn on encryption.

We say "turn on encryption" because that phrase typed into a search engine gives you good links to general instructions on encryption. (Unfortunately we can't say "turn on encryption" on Windows, because only Windows Professional offers full disk encryption.)

4.2 Pick a long password.

"Long" is more understandable than "strong." PIN is understood as the number that locks your phone, so you can extend this by including it in the same sentence to include desktop PC or laptop device logins. "Random" is a bit technical, but gets across the idea that it shouldn't just be a familiar sentence. We spend a lot of time arguing internally about whether we should say "six" or "seven"!

4.3 Don't reuse your passwords!

Reusing passwords is one of the top ways that accounts can be compromised, but it can be hard to stop doing it. One thing that can really help is to use a tool called a "password manager". There are a number of password manager guides, such as the ones on SSD. Additionally, it might sound surprising, but you can actually write down passwords and keep them in your wallet! This might seem insecure, but it's actually much better than reusing passwords. (Password reuse really is very bad.)

Why do passwords matter so much? Check out websites like https://www.HaveIBeenPwned.com/ – Password dumps affect regular people all the time.

4.4 Turn on two-factor authentication.

In an attempt to "avoid jargon," almost every web service uses a different term for two-factor authentication. We say "two-factor or two-step" to imply that it might be called a number of different things. We also give the basic reason why you should turn on two-factor authentication: it will help stop your logins and accounts from being hacked.

Understanding *why* two-factor might protect you is difficult, but getting the benefit from it is not.

For info on how to tell what accounts offer two-factor authentication, you can use websites like https://www.twofactorauth.org/. (Generally, websites like Google, Facebook, etc support it.)

4.5 Avoid clicking on strange links or email attachments.

We say this to reinforce the idea that you are most vulnerable to phishing when presented with links or attachments, but security experts have long internal debates about this advice too. Can anyone really go through life not clicking on any links or email attachments? Can anyone confidently tell when a link or attachment is "strange" (that is, a fraudulent attempt to trick you into accepting malware onto your computere)?

In concrete terms, if you receive strange attachments or links, one thing you can do is talk to the supposed sender in person or over the phone, to verify the weird email. But if you have better suggestions, go for it (and let us know!).

4.6 Use an end-to-end encrypted messenger app like Signal or WhatsApp.

Our first product mention! Break out the ™ symbols! JK. Recommending specific software or hardware is actually very complicated, but people usually want a concrete suggestion. So why Signal?

Signal was one of the first audited, open source, messaging devices with a strong theoretical cryptographic foundation, backed by an organization specifically dedicated to providing secure end-to-end encryption. It suffers from some of the problems of a small and underfunded software project, but it is reasonably safe from compromise and has a broad user base.

WhatsApp's parent company, Facebook, is not very trustworthy, but the client itself is end-to-end encrypted, and (we believe) is unlikely to be undermined without a large and highly critical expert audience spotting the problem.

By offering two alternatives, we try to imply that the important thing here is "secure messaging app" rather than a particular secure messaging app. We put this advice at the end of our list, because at this point no one will remember much beyond the brand names.

4.7 To be anonymous online, use the Tor Browser.

People are often more curious about anonymity than fighting surveillance (they are more concerned about being generally exposed online, than specifically monitored by the authorities).

Staying anonymous online involves more than just using Tor, but the Tor project does a good job of warning people who download their software about this. We try to convey that Tor is a solution for anonymity, and not one for defending against surveillance or other side-effects.

"Use Tor; Use Signal" is not always the best advice, but if you start searching for advice on Tor and Signal, there's a good chance you will be directed to more detailed guidance by experts who know what they're talking about.

5 A positive security culture for organizers

Following the uptick in alt-right activity after Charlottesville, a group called Equality Labs wrote up a guide for organizers about protecting yourself from doxxing attacks.

> *Equality Labs is a South Asian community technology organization, that works at the intersection of community-based participatory research, socially-engaged arts, and digital security. They are dedicated to ending caste apartheid, Islamophobia, and religious intolerance; and they place an emphasis on further elevating trans and cis femme voices from these communities.*

Here's what they put in the intro to their guide:

> Hey Movement Fam,
>
> It is the folks from Equality Labs and we have an urgent Anti-Doxing guide to support the activists who are getting slammed by Alt-right Forces around the country for coming out and resisting Nazis from Charlottesville to Berkeley.
>
> [...] Post Charlottesville, Boston, and the Bay Area Anti-White supremacist marches we are seeing an unprecedented number of doxing attacks on all members of the movements.[3]

"Security culture" is important for crisis times, but it's also important for the long run. Additionally, it's important to ensure that this is a positive and inclusive vision of security culture, not a toxic one. Equality Labs, collaborating with and building on work by groups like Stop LAPD Spying Coalition, have outlined such a vision.

The challenges we face (such as the escalated activity of the White Supremacists after Charlottesville, or the regular grind of state oppression) may be scary, but the best defense is one rooted in information, compassion and self-care for ourselves and each other, and a commitment to collective resilience.

What to do? What is security culture? The basic idea is to adopt best practices to stay safe. These are things that should be incorporated into your regular digital security practices, and into your regular habits more generally. The practices will help lock you down through attacks. But it's not enough to just do it once and then move on: You need to maintain these things to keep your digital resilience. *"Security is a process, not a product."*

Stop LAPD Spying Coalition talk about adopting a vision of *security culture* that centers all collective security practices as a form of expressing love and solidarity. We all have a sense of it from being marginalized, targeted, and activists. It's about harnessing those good instincts with knowledge and practice.

We can build power instead of paranoia, and meet people where they're at. From there we can have communities of practice that normalize better practices in a way that is resilient in a crisis.

Digital security is a system. You are creating and implementing it as part of your core skills as an organizer. There is no silver bullet to digital security – it is an awareness and a practice. It gets better with reiteration and with a community committed together to stay safe. The best defense is a collective one and we are all in it together. :)

[3] From the ANTI-DOXING GUIDE FOR ACTIVISTS FACING ATTACKS FROM THE ALT-RIGHT. See:
https://github.com/sptankard/digitalsecuritycurriculum/blob/master/anti_doxing_guide.md
Adapted version of guide originally published by Equality Labs, 12017 Sep 1.
https://equalitylabs.org , https://medium.com/@EqualityLabs/