WHAT IS DIGITAL SECURITY?

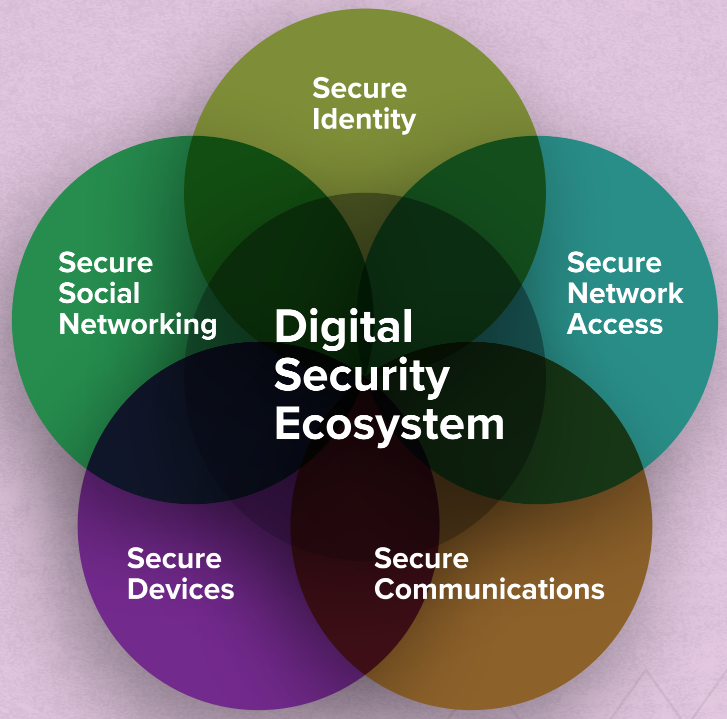
HOW TO USE THIS CURRICULUM

So, now that we know how big the problem is let's start with a definition: What the heck is **digital security** anyway?

Digital security is a set of defensive practices and awarenesses that ensures that all your devices, data, communications, and identity markers are protected to minimize surveillance by entities or individuals that may directly or indirectly wish you harm.

AN ECOSYSTEM OF DIGITAL SECURITY

Digital security is part of a large ecosystem of thinking in regards to your safety. In this ecoystem each part works with the others to secure the whole. That is why we break down our modules into easily accesible part of this ecosystem.



The digital security ecosystem includes how you secure your devices and data, the way you access your network, and the means by which you protect your identity and communications. Each part of this ecosystem can be protected or it can becompromised. Our goal is to give you the tools to better understand this ecosystem and show you ways to use more disciplined practices that will help build your digital resilence.

While we are focusing only on digital communications, we encourage everyone to also think about physical and emotional threats, it's important to consider everything and to—always plan accordingly.

It's OK if this confusing! The more you start thinking about it on your own and with trusted friends the easier it will become. Promise! So let's begin.

TIP: Individuals that love their communities practice good digital security

IT'S ALL ABOUT HARM REDUCTION RIGHT NOW

In our journey toward better digital security, it is important to keep in mind that internet security solutions, programs, and services available on the internet can change their security settings and privacy policies without notice, possibly putting users at risk. New security updates, as well as viruses and malware, are launched every day. This means that what was secure yesterday may be vulnerable to attack today.

There is no alternative to staying aware, informed, and engaged **and most importantly fighting back as a community. You are only as safe as the discipline of your digital network.**

We also know that maintaining a secure environment can be hard work. At best, you have to change passwords, habits, and perhaps the software you use on your main computer or device. At worst, you have to constantly think about whether you are leaking confidential information or using unsafe practices.

Even when you know the problems, some solutions may be out of your hands. Other people may require you to continue unsafe digital security practices even after you explain the dangers. For instance, work colleagues might want you to continue to open email attachments from them, even though you know your attackers could impersonate them and send you malware. Or, you may be concerned that your main computer has already been compromised.

And you know what? All of that is ok. In order to become a digitally resilent community together we have to be patient, firm, and aware that digital security is a journey not a destination. This is why we use the harm reduction framework.

We will make mistakes, and we will also be getting stronger together. We want to be a learning community that has patience and compassion for each other during this difficult time. So ask questions, ask them frequently, and know the work you begin today will only grow if you stay commited to digital resilence tomorrow.

SIGNS OF SECURITY COMPROMISE

Many people feel safe when, in fact, they already have a compromised digital ecosystems. Do you know what the signs of compromise could be? Here is a list of some examples:

- Passwords that change mysteriously.
- Private messages that appear to have been read by someone else.
- Websites that have become inaccessible from certain countries.
- New pop-ups constantly launch from your browser.
- Instances when your web browser redirects or crashes
- A rapid reduction of battery life, despite little-to-no use
- Instances when your cursor unexpectedly moves without your direction.
- Links from people you don't know via Facebook, Twitter, WhatsApp, or e-mail.

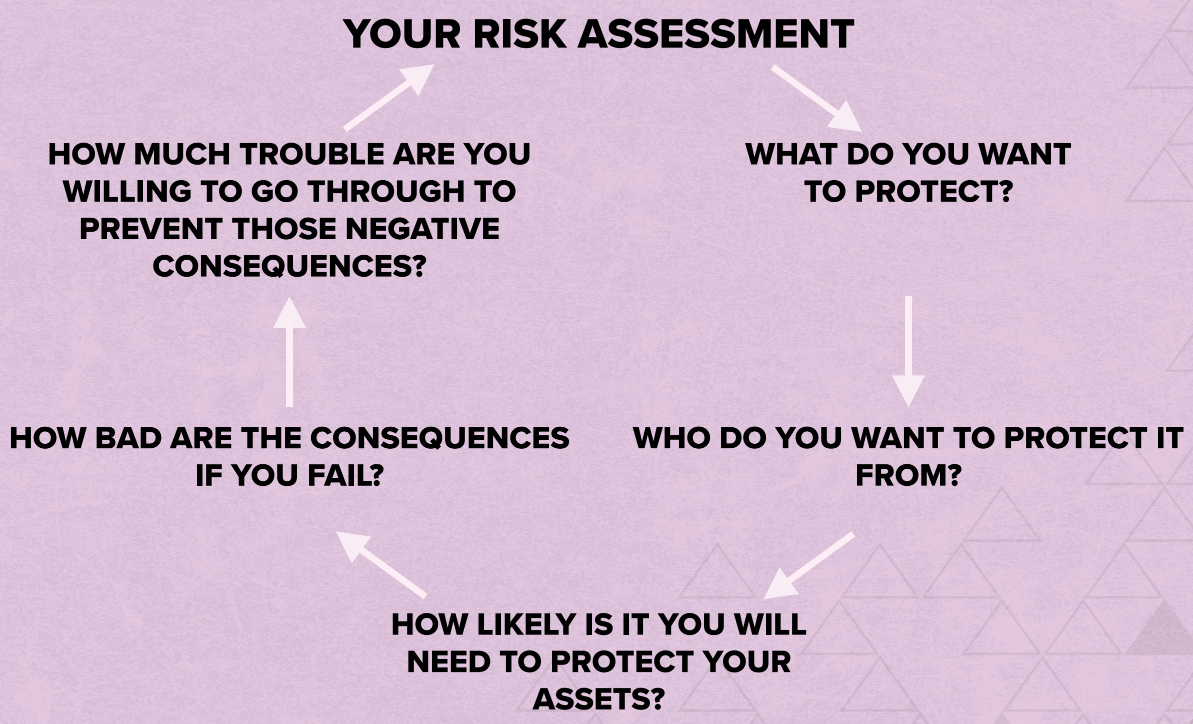
If you have any of these symptoms don't panic. Just take your device to a trusted IT professional and have them take a look. Even if you don't have a security compromise these symptoms can also sometimes point to other serious problems on your machines. The point is to be aware and be proactive about problems so when a real threat arises you are ready.

HOW TO MAKE A RISK ASSESSMENT

Risk assesment is a skill that we use in many aspects of our lives. It is what we use when we think about what side of the street to walk on at night, whether we lock our doors in our houses and the numerous other calculations we make to balance risk with the effort it takes to protect ourselves from a threat.

Digital security is no different. By thinking through and mapping out the risks we face, we can make better decisions about how to stay safe and protect our friends and networks. When you take the time to create a risk assessment model for yourself or your organization/network you can:

- Identify your risks—specifically, the people or institutions that may pose a threat—and understand the various ways they could potentially target you.
- Understand your current or future vulnerabilities so you can account for them.
- Brainstorm how the vulnerabilities of the network(s) or organizations you are part of can affect you. For example, if you don't know the technical practices of an organization or network, you may want to rethink the sensitive information you share, it may not be adequately protected.



YOUR RISK ASSESSMENT

WHAT DO YOU WANT TO PROTECT?

WHO DO YOU WANT TO PROTECT IT FROM?

HOW LIKELY IS IT YOU WILL NEED TO PROTECT YOUR ASSETS?

HOW BAD ARE THE CONSEQUENCES IF YOU FAIL?

HOW MUCH TROUBLE ARE YOU WILLING TO GO THROUGH TO PREVENT THOSE NEGATIVE CONSEQUENCES?

While you are the best person to understand your own risk, make sure to research or talk to people who have a better understanding of your adversaries' capabilities. This is especially true about digital surveillance strategies and laws that may change quickly from one day to the next.

It is important to note that in managing risks to improve security there are always trade-offs. It's impossible to being 100% secure and digital security tools alone will not make you more secure. Ultimately, you will need to think deeply about your behaviors and practices.

Ask yourself a few questions:

What do you want to protect?
What do you have that requires protection? Some examples could include: personal information, sensitive communications, statistical reports, incriminating evidence, photographs, film, documentation of a movement, or written and oral histories of our communities.

Who do you want to protect it from?
The information you have may need to be protected from right-wing adversaries, the police, intelligence officers, movement infiltrators, and the state.

How likely is it that you will need to protect your assets?
What level of protection does your information need? How often are you exposed to a threat?

How bad are the consequences if you fail?
What can happen if the information you care about "leaks"? Could you lose the information completely? What does this mean for you as an individual, our organizations, movements, and our larger community?

How much trouble are you willing to go through in order to prevent those negative consequences?
For example, are you willing to tighten the security on your devices, learn more about digital security principles and use best practices?

Ultimately, by questioning your behavior you can reduce your digital imprint along with the amount of sensitive data you post online.

Let's do a risk assessment for one of the following scenarios. Before you begin, here are some quick definitions:

- **Threat:** An entity that can cause harm.
- **Adversary:** The opposition that poses this threat.
- **Asset:** Something of value that requires protecting.
- **Risk:** The likelihood of a threat to a vulnerable asset.

Consider who may present themselves as potential adversaries:

- A roommate
- A blogger with a grudge

- An employer
- The police department through an untargeted arrest at a protest
- Police or the FBI targeting you
- The NSA targeting you

Different adversaries have different capacities and therefore require different strategies for mitigating threats. For example, your employer may not break into your home, but they can monitor you at work. Your roommate may not set up a fake cell tower but could have direct physical access to your phone. A police arrest at a protest (generally) won't lead to a warrant for your email, but the police could get it directly from your phone on site.

RISK ASSESSMENT MODEL

Read the chart below to get an idea of how to think through your threat model. Some skills you may not understand quite yet. But return to this table as a model after you have gone through our training or read this curriculum handbook. You will find your understanding will change as you gain digital surveillance literacy. Some visit this page often or better yet make your own!

THREATS	RISKS	POSSIBLE ADVERSARIES	CURRENT CAPACITIES	CAPACITIES REQUIRED
Example 1: Someone is accessing my email.	• I've already shared my password. • My password is weak and the same across multiple accounts. • I have a habit of leaving my laptop unattended.	• Roomates • "Friends" • Infiltrators	• I will change my passwords so they are strong. • I will no longer share my passwords with anyone. • I won't keep my passwords in online documents or emails.	• I need to install a password manager so I can use strong and diverse passwords for different accounts. • I need to set up two-factor

THREATS	RISKS	POSSIBLE ADVERSARIES	CURRENT CAPACITIES	CAPACITIES REQUIRED
Example 2: My mobile phone is confiscated at Trump protest.	• I have a weak password on my phone lock or use fingerprint login. • I have sensitive contacts on my phone under their real names. • I use apps like Gmail, through which anyone who has physical access to my phone can read my email without a password.	• The police. • Private security guards. • Department of Homeland Security Officials.	• I can change my password so it's stronger. • I can remove the fingerprint login so I'm not compelled to use it unwillingly. • I can use pseudonyms for sensitive contacts. • I can leave my phone at home. • I can delete non-essential apps.	• I need to encrypt my phone.

THREATS	RISKS	POSSIBLE ADVERSARIES	CURRENT CAPACITIES	CAPACITIES REQUIRED
Example 3: Someone hacking my computer.	• I don't know the various ways they can hack into my computer, and I have sensitive information stored on it.	• List anyone who would want to hack into your computer:	• I can keep my operating system and software up to date, and encrypt the hard drive. • I can store sensitive files on a password-protected USB drive.	• I need to research the various ways in which someone can hack into my computer.

NOTE: If you're working with an organization, https://safetag.org has both an action guide and a curricula on risk modeling. If you want to think more about your organization's security culture, in addition to digital security, Ruckus has a great manual: http://pdf.resistrnc.org/RuckusSecurityCultureForActivists.pdf