Follow-on Handout to Security Training Module

September 21, 2021

10AM-Noon ET

Environmental Leadership Program—Crude Accountability and FracTracker Alliance

1. Digital Tools—overview of how we protect ourselves online

   We can use specific tools on our devices to help us stay more secure. While we can have lots of tools in our toolboxes, we recommend three for this program: 1) a password safe, 2) Signal secure messaging, and 3) Protonmail encrypted email. Each of these tools is free, is easy to install on your device, and is simple to use.

   Before we get into the specifics of the three programs, I want to provide a short overview of why these security protocols and measures are important.

   Let's start with passwords. Passwords are key components in our security hygiene. The more complex our passwords are, the more difficult they are to crack, and this is the first mode of defense against hackers, malware, and those who are trying to access our information for whatever reason. So, the first step is to install a password on your phone and computer if you don't have one already.

   When you are creating a password make sure it is not easy to guess. Avoid using birthdays, addresses, pet names, etc. Some useful tips for creating (and maintaining) a safe password can be found here:
   https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

   One more suggestion is to be mindful of ways that scammers can have help in finding or guessing your passwords. Don't participate in those "quizzes" or questions on social media in which you are invited to name your favorite band or remember the name of your first pet or name your hometown. These are all excellent ways for scammers to obtain access to your personal information, which could be part of your passwords.

2. Specific Tools for use in this program:

   a. Password Safe
      As we start setting up our security protocols, one of the most important things we can do is set up a password safe, where we can keep all our passwords secure. In this way, we only have to remember one password—the password to the safe—and all the others are secure. Equally important, because we are not trying to remember a ton of passwords, we can create, more secure passwords, because they are in the safe, and not in our minds.

There are a number of good solutions for password safes, but we recommend two: Keepass and Lastpass. Keepass is a program you download to your computer, and the password safe is on your computer. As long as your computer is safe, your password safe is protected. https://keepass.info/
Lastpass is a password safe that is in the cloud. This may be a better solution for those who travel, or who are unsure about the security of their device. It is free if you use it on only one device: https://lastpass.com/create-account.php

b. Signal (phone and computer)
Signal is an encrypted text and calling app, which is much more secure than Whatsapp or Telegram, and can be easily downloaded to your phone or computer. So, why use Signal instead of Whatsapp? For starters, it is much more secure. Whatsapp has been compromised in a number of countries, resulting in activists being detained or imprisoned. And Whatsapp is owned by Facebook. We all know the questionable level of trust for security with FB, and there is little evidence that, although Whatsapp messages and calls are end-to-end encrypted while they are happening, FB is not storing the information somewhere as it does with its other data. Signal is also end-to-end encrypted, but it does not save meta-data anywhere, so the information is only between you and the person with whom you are communicating. If the two of you employ good security hygiene, your communication can be very secure.

c. Protonmail (computer)
Protonmail is a free, end-to-end encrypted email service, which you can use without having to download an application (unless you choose to have it on your phone). It was created in Switzerland and was initially set up to provide protection against both US and Russian malware. Protonmail is end-to-end encrypted, and emails are also encrypted in storage, which means even the Protonmail folks can't read your messages. Additionally, they don't track IP addresses. This is significantly safer than using Gmail, which collects meta data and is not automatically encrypted. There is an argument about hiding in plain sight, but for our purposes, working with Protonmail is highly preferable.
The overall concern with this training is about safety and security and being proactive. Having good security hygiene helps to create a less stressful work environment—one in which we are ahead of the security curve, and in our own lane, rather than trying defensively to block and avoid threats. Of course, we need to be flexible, agile, and willing to add new tools to our toolkit, but with these three initial steps, we are off to a good start.

Crude Accountability is available for private security training sessions, including download instructions, how to use tutorials, and security strategy.