DIGITAL SECURITY TOOLKIT

UNREPRESENTED
NATIONS & PEOPLES
ORGANIZATION
unpo.org

TABLE OF CONTENTS

WELCOME TO OUR DIGITAL SECURITY TOOLKIT!

WHO ARE YOU?

You are an individual or a Non-Govermental organization interested in learning more, about how to educate others and on how to protect yourselves from online threats and to learn about digital security for daily activism.

WHO ARE WE?

The Unrepresented Nations and Peoples Organization (UNPO) is an international movement and organization established to empower the voices of unrepresented and marginalized peoples worldwide and to protect their rights to self-determination. We have designed the "Digital Security Training Pack" which is also a tailor made manual to raise awareness on Cyber risks and provides tips and tricks to use internet connection more safely. In this toolkits our experts shared the basis of Cybersecurity to protect and preserve activists personal data.

WHAT WILL YOU LEARN?

This toolkit will provide activists with the necessary information to browse online while being aware of the possible cyber risks. Throughout this document, you will find tips and tricks from experts to develop your strategy to pursue your actions while being proactive in your digital journey.

GENERAL INFORMATION

The material that we have prepared for this training should be completed in 4 hours. We have divided the material into 8 parts. Each one is covering a different topic and it will be divided into different sections on what should be said, asked, showed and possible activities to be done with the participants.

WHAT DO YOU NEED?

In order to use this document appropriately, the trainer would need the PowerPoint which was created to provide further practical information as well as to share the information the most efficient way.

WHAT TO EXPECT?

In this toolkit, we have integrated short activities to assess participants in their understanding as well as consolidating the learning process.

PRACTICAL INFORMATION

PARTICIPANTS

Numbers: Trainings are usually ideal with 4-16 people. With more than 16 participants it becomes hard to manage group conversations.

Selecting people: If you know you are likely to have more than 16 people interested then you will either have to decide to run more than one training, or decide on fair criteria for how you will choose the participants. You might decide in advance that want to prioritize certain types of participants, depending on your group's needs – e.g. women, or young people. You might also decide to target people with the same level of knowledge or to mix up beginners with more experienced people. Be prepared to explain to people why they were not chosen, and why that was a fair decision. When you have decided on criteria, you will then need to work out how people will apply (e.g. online form, or by email). You will need to work out a timeline for when you will ask people to apply by, and then a deadline to let people know if they have been selected or not.

Preparation: Decide if you want to ask your participants to do any reading or thinking before they attend the training, and let them know in advance so they have time to do this.

VENUE

Size: Find a venue that will comfortably fit your training group, including trainer/s. Make sure that there is space to move around (even if that means you have to push tables and chairs around), and to break up into small groups.

Availability: Venues often get booked up, so make sure you have it confirmed before you notify participants.

Catering: It is important to have tea/coffee breaks and a lunch break on the training day. These also help participants bond and discuss what they have learned.

TIMING

Hold your training at a time and day when most people will be able to attend. This may be on a weekend, or over a series of evenings.

RESOURCES:

Look through this training pack and see what resources you will need for each session (these are indicated at the top of each session). Print out any documents that you need for sessions. If you are going to use the slideshow, make sure the venue has a projector that you can use, or arrange to hire one. Arrive early to the venue to set the projector up with your computer (remember to bring an adaptor) – this always takes more time than you think it should!

EVALUATION SESSION

When you have finished your training – even if you only did one of the four days – it is important to find out from the participants what they found useful about it, what they found was not so useful, and any suggestions they have for improving the training. This lets you know what people have learned, and how you can do it even better next time.

There are many ways of getting this sort of feedback. What is really important is doing it as soon as possible after the end of the training, otherwise, people get back into their busy lives and will not have time.

You could hand out paper forms, ask the group and write their answers on the board, or ask them by email. Ask them to think about both the content of the training and the logistics.

We suggest that you ask these questions:

- What did you find useful about the training?
- What was not so useful? What did you want more information on?
- What would your suggestions be for making this training even better?

It is also worth asking what participants thought about each session, as some sessions may have been more successful than others.

HOW TO USE THIS TOOLKIT

Say: Information that we suggest you say aloud to the group to guide them through the session

Ask: Information that we suggest you ask aloud to the group to guide them through the session

Show: The PowerPoint slide that should be presented. If you have access to a laptop and a projector, you can show it. If you don't, you can print out handouts for participants.

Activity: Activities to help participants engage and practice what they are learning
Definition: Definitions to help participants understand the concepts explained

Definition: These are definitions to help participants understand the concepts explained.

Practical tips: These are useful suggestions to improve digital security.

WELCOME AND OVERVIEW

Welcome the participants to the training and thank them for coming. Explain the purpose of the training. Explain how long the training will be and any other practical information (breaks or refreshments is available).

Ice Breaker

To make the participants more comfortable and familiarize with each other: Ask their name and something about them. What computer they use in their everyday life. What kind of phone or PC they have (without giving much details). Ask if they have ever taken any cybersecurity level course.

Show slide 1: Understanding the importance of digital security

Say: "We use digital tools for more and more everyday activities. We have seen an exponential growth in using some form of a computer (often a smartphone) for things like shopping, telling our fridge to turn on, campaigning for a cause, doing our homework or assignment - and increasingly technology is evolving so that all of this in a single networked digital society. We became so dependent on digital devices in our daily lives that we became too vulnerable to digital threats, including awsuits, extortion, hacks and much more.

Ask: Where does that leave activists? Extremely vulnerable.

Here below, a few cases of cyber attacks on activists:

- The case of the Iranian hacking group that used a driver's license training app to get to an activist. Show that hackers use personal information to obtain results including pretending to be the subject.

- In 2020, malware hidden in a driving license application was detected in Sweden. According to Amir Rashidi, a researcher at Miian group, a human rights organization with a focus on digital security, the application targets ethnic and religious minorities. When the application is installed it can record conversations, location and browser history.

Say: This course is not just to train you in becoming a digital security professional, but to ensure that you and your community of activists or people are aware of the eventual cyber risks and become proactive to tread carefully for your daily activism.

A LOOK AT SOME THEORY OF DIGITAL SECURITY

Show slide: Definition of Cybersecurity

Say: Cybersecurity is all about protecting digital assets from threats. An asset can be anything you want to protect: your physical gadgets like your phone or smartwatch that you don't want to be stolen from you at the airport. But more often than not the assets you are protecting as a cybersecurity expert is data.

Ask: What kind of skills do you think a cybersecurity person has ? Write up their answers on the board.

Show slide:

The reality is that cybersecurity is a multidisciplinary field - and unlike James Bond, you can't be an expert in everything- as it is a broad and complicated system, within the cybersecurity discipline, it includes:

- Critical infrastructure security
- Application Security
- Network security
- Cloud security
- Internet of Things (IoT) security
- And much more...

In this session, we will not go into each of these sub-discipline of Cybersecurity, but instead, you will have a better understanding of the whole discipline which will enable you to address the relevant people for your concerns.

Ask: What is the difference between data and information?

The hacker often is not concerned by processing the data. Like the cybersecurity expert, he isn't James Bond, he doesn't do multiple tasks, his job is to extract data and then either hand it over to his overlords for processing or sell it to someone else for processing. So when I speak about data, think of it as raw information that hasn't been treated. Once you understand the importance of assets, and particularly data protection, let us have a look at the CIA triad of data, not to confuse with the Central intelligence Agency.

CIA Triad or Confidentiality, Integrity and Availability Triad is a security model designed to guide people and policies for information security.

Show slide: Confidentiality, Integrity and Accessibility

Confidentiality: keeping data secure from willing or unwilling attempts to access it to view it.
Integrity: making sure that data is not modified willingly by any actors
Accessibility: Making sure your data is accessible at all times and easily, with respect to its integrity too

Ask: what's the difference between Security and Privacy in digital security?

Privacy refers to your ability to control, access, and regulate your personal information or the information of the organization you work for.

Security refers to the entire system that protects data from threats.

You can be in an incredibly secure environment with poor privacy because your data will still remain integral and won't be stolen, but the provider could take a peek at it at any time.

Let's do an exercise that constitutes the essence of cybersecurity analysis, that is defining your assets, your adversaries, the resources at your disposal, the likelihood of attack and your abilities.
A final framework of analysis :

Ask: The participants to go throw the following questions about their digital set up and which actors they have to beware of.

- Assets : What do I have to protect?
- Adversary : From whom?
- Resources : What resources does my adversary have?
- Likelihood : What is the likelihood of my adversary will target me?
- Ability : How far will I go to protect my assets?

PROTECTING YOUR DATA ON YOUR PC AND PHONE

A) Passwords

A password is a secret word or phrase that must be used to gain admission to a place. (1)

The number one form of protection for your data is your user password to enter your device. This inevitably creates a whole discipline of how to create elaborate methods to encrypt and decrypt data and messages in order to keep them hidden. This discipline is known as cryptography, has existed for thousands of years, and is essential to understand cybersecurity. Whilst we won't delve into the complex mathematical problems cryptography produces, we will ask ourselves what makes a good password.

Ask the audience : What makes a good password? What makes a bad password?

Possible answers :

Nothing that relates to your personal life (e.g. the name of your dog or favorite soccer team) Nothing that is one or two words only, as these are often Different characters like caps lock numbers or symbols Unintelligibility? Safely stored and secured! A good password still may have to be memorable

Show

REALLY BAD	BETTER	EXCELLENT!
password	Cynthis19070!	j5Lyf*H6llg
admin	LayC70!	7+n*7XonG5
cynthia	*cynthia70lay	VJ(>0WuvE83V
cynthialay	CynthisL7019	R.xzVv2m0R0

[1] Cambridge dictionary

WHAT MAKES A GOOD PASSWORD?

1. Length

Say : the most important variable in determining password strength is length. This is by far the most important variable and should be hammered home to anyone when determining their password. Having a sentence as your password that is long is safer than just a 5 character password full of different characters. One is because having a long password can put off a hacker through pure security theatre. The other is that if the hacker is using an AI to try and "blunt force" open your hard drive they likely will find it much easier to crack open the 5-character password.

2. Complexity

Say : Most of us, when creating a password, we often use words and maybe numbers. But these passwords are easier and easier to crack due to new software and tools which instantaneously checks all known words. These software often use AI (artificial intelligence). Hence why it is always better to have a serie of random letters rather than a word.

3. Special of Character

Say : Use a Special character like: @ $ % & make the password extra secure and harder to guess. Nowadays, some websites require you to use a special character to validate your password but unfortunately not all.

Say : The worst password you can use is a single word. Starting from there, a hacker can use what is called a dictionary attack to crack your passwords. A dictionary attack can work on a word. As well as birthdays, names or even "123456789".

The biggest issue we have is that in the modern era, we have many passwords for many different accounts and our own devices. In addition, if you have sensitive information you want to encrypt your hard drive and cloud storage with a nice, strong 36-character password that you will likely not remember easily. The solution to this problem is using a password manager.

B) Password manager

A password manager allows individuals and businesses to save and manage all their passwords from one safe space. Thus, users will no longer be required to remember multiple passwords. (2)

The difference between password managers can vary in price range, but also where your passwords are actually stored. Bitwarden for example stores your passwords relatively safely in a cloud on their servers and allows for several people to have access to different accounts. But you may not trust Bitwarden for whatever reason and want to store your data locally. KeyPassXC is a good example of a locally stored password manager.

Having a passphrase to easily memorize access to your password manager is important, but let's have a look at another layer of security you can implement: 2FA

C) 2 factor authentication

Two Factor Authentication, or 2FA, is an extra layer of protection used to ensure the security of online accounts beyond just a username and password. (3)

You can authenticate through 2 methods:

- Something you know (like the password)
- Something you own or is on you (biometric)

The good news is that you can and should use both. With 2-Factor Authentification you can ensure that even if a hacker cracks your password you have that extra layer of security. This often comes in the form of:

- An app on your phone that gives a temporary code to access the service (see: Google Authenticator)
- A USB key like Yubikeys or Nitrokeys that when plugged in can either give you access to codes above or through your touch or even fingerprint enable you to access your account.

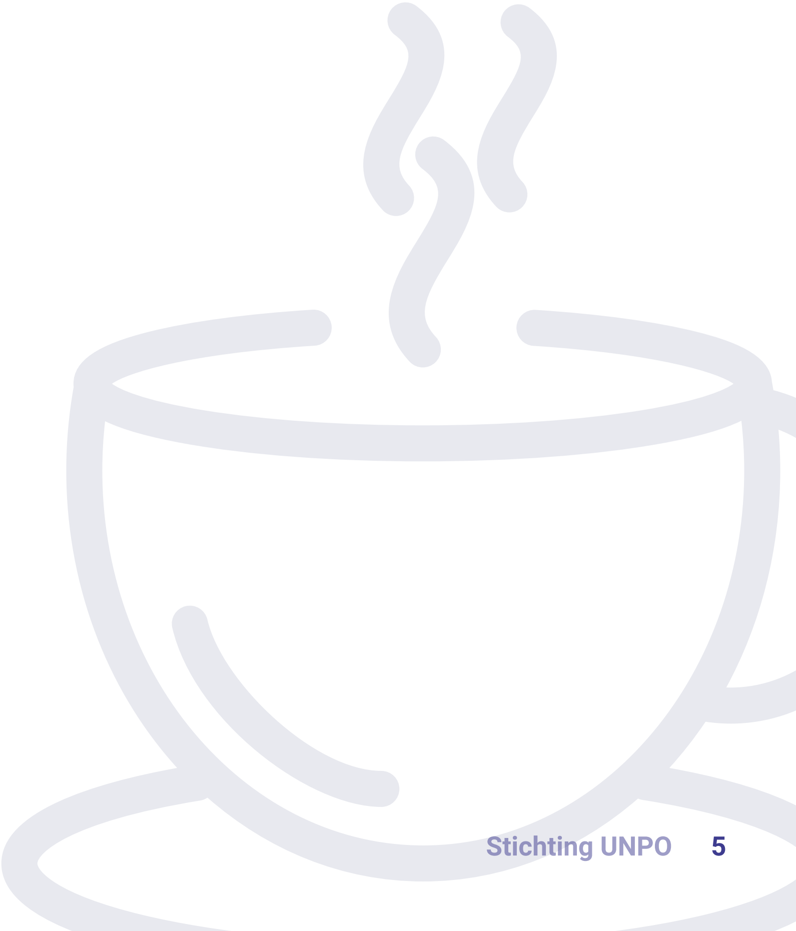
2FA is fast becoming a bread-and-butter measure in digital security. Most social media accounts allow for 2FA now and you should implement a 2FA system on most of your email, messaging, and social media accounts the moment you leave this class if you think you can have access.

Protecting Hard Drive and Cloud Storage Systems: In addition to encrypting your hard drive, consider using an external hard drive for Cloud systems that are verified like Google Cloud, OneDrive, etc.

2 Zoho.com

3 Authy.com https://authy.com/what-is-2fa/

BREAK



BROWSING THE INTERNET CONFIDENTIALLY

Having knowledge of the following is essential before starting to browse securely :

- Who is your Internet Service Provider?
- What is the nature of your IP address? Is it fixed or does it change? Your IP address is like your identifier for your home or work network.
- What are your firewall settings, that regulate your IPs relationship with all the other Ips that constitute the world wide web (think of it as a border control policy for who comes in and out)?

A) Using a VPN

? **Ask**: can anyone explain to me what a VPN is?

Say: A VPN or Virtual Private Network connects your computer to another server and then accesses the internet through it, hiding your activity. It also can sometimes "spoof" your location allowing you to circumvent geolocation blocks.

Note however that a VPN does not protect you from an internet shutdown, as your IP will still be "active" during an internet shutdown trying to access the VPN, and this leaves you vulnerable! Good VPNs include NordVPN or Mullvad, but in general, you also want a VPN that doesn't record logs as that essentially only transfers it from your Internet Service Provider to the VPN provider who can then either sell or misuse that data.

B) Web browsers

? **Ask:** what web browsers do you all use?

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Brave? Vivaldi?

In general, it's good to have 2 web browsers, one that had had your accounts and is synced for professional or private work use, and another to simply search for something. This is because search engines track your search history and modify your browsing experience. Mozilla Firefox and Vivaldi are generally safe browsers. Chrome and MS Edge are designed by big software developers who want to grab your data and use it for commercial reasons. You can get what is called unGoogled Chromium which is open source and removes all of Google's built-in data mining (5). Brave also has some built-in analytics but has some very strong security features. Totally unsafe browsers for human rights activists include Opera (whose data goes straight to a Chinese server) but also built-in browsers that are designed by adware companies.

4 A firewall configuration is a collection of profiles or rules. You apply these profiles or rules on the computer to determine the permissions for all inbound and outbound connections for specific ports. (IBM.com) 5 Data mining is the practice of analysing large databases in order to generate new information

PROTECTING YOU FROM PHISHING AND MALWARE

Phishing: “The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers”(6). Malware: “It is a software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system”(7).

Say: Phishing attacks are often associated with e-mail but they are actually also present in all other walks of communication. The idea of phishing is that you present bait by pretending to be a trusted person. You may have heard about phishing. A lot of phishing is done via email these days but you may have also heard of catfishing, using dating apps. And in the old days, you would have conmen calling people over the phone. A hacker who uses phishing is someone who is attempting social engineering, and the better they are at social engineering the worse damage they can inflict to you.

Let's have a look at some messages that contain links that could be phishing :

Show slides with examples and how they could be identified.

Say: The idea here is if you find a link like this you need to be able to create an environment where clicking on it and downloading it will isolate any potential malware on it. This is known as sandboxing and it's a crucial concept in cybersecurity. The old way of sandboxing was simply having an offline computer, working on that, and ensuring it had no ability to connect to the internet. Increasingly though you can sandbox by setting up a Virtual Machine. A virtual machine is like one of those Russian dolls that unpack itself: it creates an operating system within an operating system.

Lastly, if you are particularly vulnerable and constantly receive loads of potential malware from your email, the websites you visit or your messaging service – and are really excited about cybersecurity, have a look into operating systems that employ sandboxing as a principle. An example is QubesOS, which makes it so that you can create different “environments” that are incapable of communicating with each other.

[6] Oxford Dictionnary
[7] Oxford Dictionnary

ENSURING YOUR COMMUNICATION IS SECURE

Ask : why is the text messaging system not secure in a country like Iran?

Say: Mobile services and Internet Service Providers in dictatorships often centralize the data that comes in and out of your phone via the services you use such as SMS. That's why using end-to- end encryption is so important.

End-to-end encryption or (E2EE) is a security method that keeps your chats and messages secure. It is the idea that two or more people have a public key and a private key.

The public key is available to anyone who requests it and your private key decrypts other public keys. To help you understand end-to-end encryption here is a helpful video

Say: Now all of you I assume use email and it's fairly ancient technology when compared to WhatsApp, Instagram, Snapchat, and other safer messaging apps we've looked at. That's why it's vital you understand what email provider to use, what kind of threats exist, and where to look for additional resources.

E-mail accounts use domains like @gmail.com to indicate which servers you are using to transmit a message via the internet. Often your work email will use your work servers and have the @organisationname.com. Most email accounts are managed by an email service provider like Google or Microsoft.

One of the key threats in addition to phishing is domain spoofing.

Domain spoofing is trying to use your domain and identity as an organization or even individual in order to have your email hijacked or simply to obtain information whilst posing as you.

To combat domain spoofing is to report End-to-end encryption on email is also a useful tool when exchanging information or a file that is sensitive. Email providers like Gmail and outlook do not come in out of the box with end-to-end encryption. For Gmail though there is an extension you can install called Mailvelope that can encrypt. Email providers that use end-to-end encryption and even have tools to allow only the recipient to decrypt a message even if they do n t have your public key include Protonmail and Tutanota. The disadvantage is that these tend to have compatibility issues with mail clients and are closed-source environments with very nascent features compared to Gmail and Outlook, but they are definitely worth looking into for specialized use.

SMARTPHONE SECURITY

? **Ask:** for a quick survey of who uses which phone Operating System (iOS vs Android)

Say: We have talked briefly about messaging apps on your phone, but the advent of smartphones has produced multiple other challenges to cybersecurity experts. One is that pretty much your whole life can now be found on your phone, and as we detailed at the start of the class.

Say: The Pegasus scandal8 showed that even democratic governments were ready to spy on citizens and did so using the phishing methods we have seen above (via a text message). Many of you may have already thought that the NSA, GCHQ and other assorted Signals Intelligence companies were already spying on you. But the reality is that before Pegasus these groups could only really read your communication between yourself and a third party. The post-Pegasus world is scary because now your entire phone can be monitored and thus any good hacker could potentially use a tool to obtain enough information on you for you to be vulnerable to threats.

The unleashing of malware like Pegasus provides the hacker access to all of your phone, making it especially illegal. But more importantly, what this shows is that our phones are very easily turned into portable surveillance devices. And you can add the fact that Google, Apple and other mobile services collect data from you for commercial reasons that can then be used against you should this data fall into the wrong hands.

Luckily there does exist a series of alternatives for those who don't want to be vulnerable using a smartphone. Graphene OS and Lineage OS are examples of what we call forks of Android code that have taken out all the services relating to Google. You can also look at phone operating systems that can effectively use sandboxing to make sure that any apps you install are not spying on others.

Beware though that in general your phone is the perfect tool to spy on you. From the hardware drivers to the gaming apps you download, most of the technology on your phone is closed-source: you don't know what code the developer has put on your phone. As we evolve into a more smartphone and tablet-dominated digital environment, your best bet as a human rights activist is to use these tools as sparingly as possible or with very specialized software.

8 Which is a scandal of allegations that spy software known as Pegasus may have been used to carry out surveillance on journalists, activists and perhaps political leaders in Spain

SOME FINAL TIPS AND FAQ

Say : Let's move on to some Frequently Asked Questions that maybe some of you can help me answer, and then do a small workshop where you ask me

Ask: Should I install an anti-virus? If so which one?

Say: Anti-viruses are often built into the operating systems now. Gone are the days when Windows would rely on third party anti-virus providers to do a lot of the heavy lifting against malware. Apple and Linux tend to be very strong against malware, the latter due to its Open Source philosophy. Open Source remember means the code is open to everyone and usually audited by other coders to confirm its integrity. Nevertheless, if you see an anti-virus installed or want to buy one, anti-viruses are generally data analytical tools that monitor where your PC is using resources and how, what files seem corrupted or otherwise suspicious and also can help you strengthen your firewall - the wall that blocks bad actors from entering your network/IP address. A good anti-virus is Bitdefender, but if you learn how to sandbox and use common sense anti-virus policies you don't need it.

Ask: Is Apple really safer than Windows?

Say: It is, but it is still subject to vulnerabilities. Choosing the right Operating System for the right kind of work you are doing is essential too. There exist so many free Linux Operating Systems that are considered much safer and secure compared to Apple and Microsoft's offerings but maybe require a bit more technical mastery. But if you are going to get into cybersecurity learning about how Linux operating systems work, ethical hacking through Kali Linux, and just the core differences in Operating Systems for both servers and personal uses is essential.

Ask: Where can I start if I want to go further into cybersecurity.

Say: As said before there are many domains you can enter in the cybersecurity field. A good start is learning the basics of hardware and software programming so that you are at least literate in the relationship between the two and then learning how to set up your own server.

Ask: How do I know if my PC or phone has been hacked?

Say: As said before, you often won’t realize you have been hacked before it's too late as hackers tend to operate in the back end of your operating system (accessing files without you noticing).

For PC, you can run checks on suspicious files using the following websites :

- For phones, there are some great tools out there now to see if you have been affected by spyware or malware: https://www.malwarebytes.com/
- For specific accounts, you can check if you have been subject to a data leak or hack through this website: https://haveibeenpwned.com/
- For email or your personal website in particular, you can check if your domain has been spoofed through looking at the domain: https://mxtoolbox.com/

Ask: What are some resources if I need help a s a Human Rights activist?

- AccessNow
- Amnesty Tech
- Center for Digital Resilience
- UNPO

Then lead a workshop with more individual cases based on the audience and what devices they have on hand.

NOTES

The Hague
Fluwelen Burgwal, 58
2511CJ, The Hague
Netherlands
unpo@unpo.org

Geneva
UNPO c/o Ecumenical Centre -
Kyoto Building
Office E 381
Chemin du Pommier 42
1218 Le Grand Saconnex
Geneva, Switzerland
geneva@unpo.org

Brussels
Rue de Trèves 49/51
Box 18, Brussels, B-1040, Belgium
unpo.brussels@unpo.org

/UNPOintl @UNPOintl @UNPOintl /UNPOintl

UNPO

UNPO

UNREPRESENTED
NATIONS & PEOPLES
ORGANIZATION
unpo.org