پەکی ڕاهێنانی

ئاسایشی(ئەمنییەت) دیجیتاڵ

UNREPRESENTED NATIONS & PEOPLES ORGANIZATION
unpo.org

پەکی ڕاهێنانی
ئاسایشی(ئەمنییەت) دیجیتاڵ

GENERAL INFORMATION

Time:

We have prepared this training material to be completed in 4 hours.

What 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.

Activities:

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

Purpose:

This toolkit will provide activists with the necessary information to browse online while being aware of the possible cyber risks. Throughtout 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.

For who:

This module is intended for Non-Governemental Organisation of individual activists which wishes to learn about digital security for their daily activism.

HOW TO USE THIS TOOLKIT

Say or Ask

Show

Activity

Definition

Practical Tips

زانیاری گشتی

کات:

ئەم ڕاهێنانەمان بۆ ئەوەی لە ماوەی ٤ کاتژمێردا تەواو بێت ئامادە کردووە.

پێداویستییەکان:

بۆ ئەوەی ئەم بەڵگەنامەیە بە شێوەیەکی گونجاو بەکاربهێنرێت، ڕاهێنەر پێویستی بە پاوەرپۆینت دەبێت کە بۆ پێدانی زانیاری زیاتری پراکتیکی و هەروەها بۆ هاوبەشکردنی زانیارییەکان بە باشترین و کارامەترین شێوە دروستکراوە.

چالاکییەکان:

لەم ئامرازەدا ئێمە چالاکییە کورتەکانمان بۆ هەڵسەنگاندنی بەشداربووان لە تێگەیشتنیان و هەروەها فێربوونی باشتر و قوواڵتر، یەکخستووە.

مەبەست و ئامانج:

ئەم ئامرازە زانیاری پێویست دەدات بە چالاکوانان بۆ ئەوەی لە هەمان کاتدا کە بە شێوەی نۆنلاین دەگەڕێن، ئاگاداری مەترسییە ئەگەرییەکانی سایبێری بن. لەم پەکەیجە دا ئێوە فێڵ و ئامۆژگارییەکانی پسپۆڕان بۆ پەرەپێدانی ستراتێژییەکەتان بۆ بەدواداچوونی چالاکییەکانتان لە گەشتی دیجیتاڵی ڕۆژانەتاندا دەبینێوە.

بۆ کێ:

ئەم پەکەیجە بۆ چالاکوانانی ڕێکخراوە ناحکومییەکانە کە بۆ چالاکی ڕۆژانەیان هیوای فێربوونی ئەمنییەت و ئاسایشی دیجیتاڵیان هەیە.

چۆن ئەم ئامرازە بەکاربێنین

بڵێن یان بپرسن

نیشاندان

چالاکی

پێناسە

ئامۆژگاری پراکتیکی

Table of Content

خشتەی ناوەڕۆک

Part 1 : Welcome and Overview

Welcome

Welcome people to the training, thank them for coming

Icebreaker: Ask people

- their names
- What they use their computer for in everyday life
- What kind of Phone and PC they have (without giving too much detail)
- Ask if they have ever taken any cybersecurity level

Show Slide 1 : Understanding the importance of digital security in the modern era

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 bacame so dependent on digital devices in our daily lives that we bacame too vulnerable to digital threats, including awsuits, extortion, hacks and much more.

Ask: Where does that leave activists? Extremely vulnerable.

Here below, few cases of cyber attacks toward activists:

- Present the case of the Iranian hacking group that used a drivers licence training app to get to an activists. 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, 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 courses 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.

Part 2 : A look at some theory of digital security

بەشی یەکەم : بەخێرهاتن و تێڕوانینێکی گشتی

بەخێربێن
بەخێرهاتنی خەڵک بۆ مەشقەکان، سوپاس بۆ هاتنیان

بۆ دەسپێک: **لە ئامادەبوان بپرسن:**
- **ناوەکانیان**
- **لە ژیانی ڕۆژانەدا کۆمپیوتەرەکەیان بۆ چی بەکاردەهێنن**
- **چ جۆرە مۆبایل و کۆمپیوتەرێکیان هەیە (بەبێ ئەوەی وردەکاری زۆر بدەن)**
- **بپرسن کە ئایا تا ئێستا هیچ ئاستێک لە ئاسایشی سایبێریان وەرگرتووە؟**

سلایدی یەکەم پیشان بدەن: **تێگەیشتن لە گرنگی ئاسایشی دیجیتاڵی لە سەردەمی مۆدێرندا**

بڵێن: **"ئێمە ئامرازە دیجیتاڵییەکان بۆ چالاکیی ڕۆژانەی زیاتر و زیاتر بەکاردەهێنین. ئێمە گەشەیەکی بەرچاومان بینیوە لە بەکارهێنانی هەندێک جۆری کۆمپیوتەر (زۆرجار مۆبایلێک) بۆ شتەکانی وەک شت کڕین ، بە یەخچاڵەکەمان (سەلاجەکەمان) بڵێین ڕۆشن بە (دابگیرسێنە)، کەمپەینکردن بە هۆیەک، ئەنجامدانی ئەرکی ماڵەوە یان ئەرکی دیکە - و تادێت تەکنەلۆژیا لە یەک کۆمەڵگەی دیجیتاڵیدا پەرەدەستێنێت. ئێمە لە ژیانی ڕۆژانەماندا ئەوەندە وابەستەی ئامێرە دیجیتاڵییەکان بووین کە زۆر بەرەوڕووی هەڕەشە دیجیتاڵییەکان، وەک تاوانبارکردن، زەوتکردن، هاککردن و زۆر شتی تر دەبینەوە.**

بپرسن: **ئەوە چالاکوانان لە کوێ جێدەهێڵێت؟ لەڕادەبەدەر لاوازە.**

چەند حاڵەتی هێرشی سایبێری بەرامبەر بە چالاکوانان لێرەدا لە خوارەوە هاتووە:

- **کەیسی گروپی هاککردنی ئێرانی بخەنەڕوو کە ئەپی (drivers licence training)یان بۆ گەیشتن بە چالاکوانێک بەکارهێناوە. نیشان بدەن کە هاکەرەکان بۆ ئەم ئامانجە، زانیاری کەسەکان بەکاردەهێنن، و هەروەها وا خۆیان نیشان دەدەن کە بابەتەکە و کەسەکەن.**

- **لە ساڵی ٢٠٢٠دا، بەرنامەیەکی زیانبەخش کە لە بەرنامەی driving license شاراوەتەوە لە سوید دۆزرایەوە. بە گوتەی ئەمیر ڕەشیدی، توێژەر و ئەندامی گروپی میان، کە ڕێکخراوێکی مافی مرۆڤ لە بواری ئاسایشی دیجیتاڵیدایە، ئەپڵیکەیشنەکە کەمینە ئەتەوەیی و ئایینییەکان دەکاتە ئامانج. کاتێک بەرنامەکە دامەزرا دەتوانێت گفتوگۆکان و شوێن و مێژووی وێبگەڕەکان تۆمار بکات.**

بڵێن: **ئەم خولە تەنها بۆ ڕاهێنانی ئێوە و کردنتان بە کەسێکی پسپۆڕ و لێهاتوو لە بواری ئاسایشی دیجیتاڵی، بۆ دڵنیابوونە لەوەی کە ئێوە و کۆمەڵگەی چالاکوانان یان هاوواڵتیانتان ئاگاداری مەترسییە سایبێرییەکانن بۆ ئەوەی بە وریاییەوە بۆ چالاکی ڕۆژانەتان هەنگاو بنێن.**

بەشی دووەم : چاوخشاندنێک بە هەندێک تیۆری ئاسایشی دیجیتاڵی

Show slide x : 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 stolen from you at the airport. But more often than not the assets you are protecting as a cybersecurity expert is data.

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

Show Slide x

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 discpline, 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-discpline of Cybersecurity, but instead you will have a better understanding of the whole discipline which will enable you to adress the relevant people for your concerns.

Ask the audience : 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 asset, and particularly data protection, let us have a looks 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.

سلایدی x پیشان بدەن : پێناسەی ئاسایشی ئێلێکترۆنی

بڵێن : ئاسایشی ئەلیکترۆنی، پاراستنی سەروەت و سامانی دیجیتاڵی لە هەڕەشەکانە. سەرمایە دەتوانێت هەر شتێک بێت کە بتانەوێت بیپارێزن : ئامێرە فیزیکییەکانتان، وەک مۆبایلەکەتان یان کاتژمێرە زیرەکەکەتان کە ناتانەوێت لە فڕۆکەخانە لێتان بدزرێت. بەڵام زۆرتر ئەو سەروەت و سامانانەی کە ئێوە وەک پسپۆڕێکی ئاسایشی ئەلیکترۆنی دەپارێزن داتاکانن.

لە ئامادەبووان بپرسن : پێتان وایە کەسێکی ئاسایشی ئەلیکترۆنی(ئەمنییەتی سایبێری) چ جۆرە لێهاتوویییەکی هەیە ؟
وەڵامەکانیان لەسەر تەختەکە بنووسن.

سلایدی x پیشان بدەن

راستییەکە ئەوەیە کە ئاسایشی ئەلیکترۆنی بواریکی فرە پسپۆرییە - و بە پێچەوانەی جەیمس بۆند، ئێوە ناتوانن لە هەموو شتێکدا شارەزا بن- بەو پێیەی سیستەمێکی فراوان و ئاڵۆزە، لەناو دیسیپلینی ئاسایشی ئەلیکترۆنیدا، بریتییە لە:

- ئاسایشی ژێرخانە گرینگەکان
- ئاسایشی بەرنامە
- ئاسایشی تۆڕ(شەبەکە)
- ئاسایشی هەور
- ئاسایشی ئینتێرنێتی شتەکان (IoT).
- هەروەها زۆر زیاتر...

لەم دانیشتنەدا، ئێمە ناچینە ناو هەریەکێک لەم بەشە لاوەکیانەی ئاسایشی ئەلیکترۆنی، بەڵکوو ناوبردنیان بۆ ئەوە بوو لە تەواوی دیسیپلینەکە تێگەیشتنێکی باشترتان ببێت کە وا دەکات بتوانن قسە لەگەڵ کەسە پەیوەندیدارەکان بکەن بۆ نیگەرانییەکانتان و ئاگاداریان کەنەوە.

لە ئامادەبووان بپرسن : جیاوازی نێوان داتا و زانیاری چییە؟

زۆرجار خەمی هاکەرەکە پرۆسێسکردنی داتاکان نییە. وەک پسپۆری ئاسایشی ئەلیکترۆنی جەیمس بۆند نییە، چەندین ئەرک ناکات، کاری ئەو دەرهێنانی داتاکانە و دواتر بۆ پرۆسێسکردن یان ڕادەستی ئاغاکانی دەکات یان دەیفرۆشێت بە کەسێکی تر بۆ پرۆسێسکردن. بۆیە کاتێک باس لە داتا دەکەین، وەک زانیارییەکی خاو بیری لێبکەنەوە کە مامەڵەی لەگەڵ نەکراوە.

کاتێک لە گرنگی سەروەت و سامان و بە تایبەتی پاراستنی داتا تێگەیشتین، با چاوێک لە داتاکانی سێگانەی سی ئای (CIA) بخشێنین، بۆ ئەوەی لەگەڵ دەزگای هەواڵگری ناوەندی تێکەڵ نەبین.

سێیەمی سی ئای ئەی یان سێگانەی نهێنی، یەکپارچەیی و بەردەستبوونی مۆدێلێکی ئەمنییە کە بۆ ڕێنماییکردنی خەڵک و سیاسەتی ئاسایشی زانیاری دارێژراوە.

Show Slide 3 : Confidentiality, Integrity and Accessbility

- **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 organisation 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 peak at it at any time.

ACTIVITY : 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?

Part 3 : Protecting your data on your PC and phone.

A) Passwords

سلایدی سێیەم پیشان بدەن : نهێنی، یەکپارچەیی و دەستڕاگەیشتن

- **نهێنی** : پاراستنی زانیاریەکان بە پارێزراوی لە هەوڵی خوازراو یان نەخوازراو بۆ دەستگەیشتن پێیان و بینینیان.
- **یەکپارچەیی** : دڵنیابوون لەوەی کە داتاکان لەلایەن هیچ ئەکتەرێکەوە دەستکاری ناکرێن
- **دەستڕاگەیشتن**: دڵنیابوون لەوەی کە داتاکانتان لە هەموو کاتێکدا و بە ئاسانی لەگەڵ ڕێزگرتن لە یەکپارچەییەکەی، لەبەردەستن.

بپرسن : جیاوازی نێوان ئاسایش و پاراستنی نهێنی لە ئاسایشی سایبێریدا چییە؟

نهێنی ئاماژەیە بۆ توانایی ئێوە بۆ کۆنترۆڵکردن، دەستگەیشتن و ڕێکخستنی زانیارییە تاکەکەسییەکانتان یان زانیارییەکانی ئەو ڕێکخراوەی کە کاری بۆ دەکەن.

ئاسایش ئاماژەیە بۆ تەواوی ئەو سیستەمەی کە داتاکان لە هەڕەشەکان دەپارێزێت.

دەتوانن لە ژینگەیەکی پارێزراوی ناباوەڕدا بن و تایبەتمەندی (privacy) خراپی هەبێت چونکە ئەگەرچی داتاکانتان یەکگرتوو دەمێننەوە و نادزرێن، بەڵام دابینکەرەکە دەتوانێت لە هەر کاتێکدا شتێکی لێ بەدەستبهێنێت.

چالاکی : با مەشقێک (چالاکییەک) بکەین کە جەوهەری شیکاری ئاسایشی ئەلیکترۆنی پێکدەهێنێت، کە ئەویش پێناسەکردنی دارایییەکانتان، نەیارەکانتان، ئەو سەرچاوانەی لەبەردەستتاندان، ئەگەری هێرشکردن و تواناکانتانە.

چوارچێوەیەکی کۆتایی شیکاری :

پرسیار بکەن : بەشداربووان بەدوای پرسیارەکانی خوارەوەدا بچن کە دەربارەی ڕێخستنی دیجیتاڵە و بزانن کە دەبێت ئاگاداری کام ئەکتەر بن.

- دارایی : چیم هەیە بیپارێزم؟
- نەیار : لە کێوە؟
- سەرچاوە : نەیارەکەم چ سەرچاوەیەکی هەیە؟
- ئەگەر : ئەگەری ئەوە چەندە کە نەیارەکەم من بکاتە ئامانج؟
- توانا : تا چەندە دەتوانم دارایییەکەم بپارێزم؟

بەشی سێیەم : پاراستنی داتاکانتان لە کۆمپیوتەر و مۆبایلەکەتاندا.

آ) نهێنوشە

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:

Good & Bad Passwords

REALLY BAD	BETTER	EXCELLENT!
password	Cynthia1970!	j5LyF*H6IIg
admin	LayC70!	7+n*7XonG5
cynthia	*cynthia70lay	VJ(>0WuVE83V
cynthialay	CynthiaL7019	R.xzVv2m0R0;

What makes a good password?

i. Lengh

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

1 Cambridge dictinary

نهێنوشە وشەیەکی نهێنی یان دەستەواژەیەکە کە دەبێت بۆ چوونەژوورەوە یان وەرگریران لە شوێنێک بەکاربهێنرێت.[1]

فۆرمی ژمارە یەک بۆ پاراستنی داتاکانتان، بۆ وەرگیران لە شوێنێک یا چوونە ژوورەوەی ئامێرەکەتان، نهێنوشە و ناوی بەکارهێنەرەکەتانە. ئەمەش بە ناچاری تەواوی ئەو دیسیپلینە دروست دەکات کە بۆ ئەوەی بە شاراوەیی بمێنێتەوە، چۆن شێوازی ورد و درشت بۆ کۆدکردن و کۆدکردنەوەی داتا و پەیامەکان دروست بکات. ئەم دیسیپلینە بە کریپتۆگرافی ناسراوە، هەزاران ساڵە بوونی هەیە و بۆ تێگەیشتن لە ئاسایشی ئەلیکترۆنی پێویستە. لە کاتێکدا ئێمە قوڵ نابینەوە لەو کێشە بیرکارییە ئاڵۆزانەی کە کریپتۆگرافی بەرهەمی دەهێنێت، بەڵام لە خۆمان دەپرسین کە چی نهێنوشەی باش دروست دەکات.

لە ئامادەبووان بپرسن : چی وا دەکات نهێنوشە باش بێت؟ چی وا دەکات نهێنوشە خراپ بێت؟

وەڵامە ئەگەرییەکان :

- هەر شتێک کە پەیوەندی بە ژیانی تایبەتی خۆتەوە هەبێت (بۆ نموونە ناوی سەگەکەتان یان تیپی تۆپی پێی دڵخوازتان)
- هەر شتێک کە تەنها یەک یان دوو وشە بێت، هەروەک چۆن زۆرجار هەن
- پیتە جیاوازەکان وەکو کاپەکان ژمارە یان هێماکان
- ناڕوونی؟
- بە سەلامەتی هەڵبگیرێت و پارێزراو بێت!
- ڕەنگە نهێنوشەی باش ئەوەیە کە لەبیر بمێنێنەتەوە.

نیشاندان:

Good & Bad Passwords

REALLY BAD	BETTER	EXCELLENT!
password	Cynthia1970!	j5LyF*H6IIg
admin	LayC70!	7+n*7XonG5
cynthia	*cynthia70lay	VJ(>0WuVE83V
cynthialay	CynthiaL7019	R.xzVv2m0R0;

چی وا دەکات نهێنوشە باش بێت؟

درێژیی .

بڵێن : گرنگترین گۆڕاو یا فاکتەر لە دیاریکردنی هێزی نهێنوشە درێژییە. ئەمە تا ئاستێکی زۆر گرنگترین فاکتەرە و دەبێ لە کاتی دیاریکردنی نهێنوشە تا ئاستێکی زۆر گرنگی پێبدرێت. هەبوونی ڕستەیەکی درێژ وەک نهێنوشە سەلامەتترە لە نهێنوشەی ٥ پیتی پڕ لە پیتی جیاواز. یەکێکیان لەبەر ئەوەیە کە هەبوونی نهێنوشەی درێژ دەتوانێت لە ڕێگەی شانۆی ئاسایشی پاکەوە هاکێرێک دوابخات یا ڕابگرێت.

1 فەرهەنگی کامبریج

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.

ii. Complexity

Say: most of us, when creating a password, we often use a words and maybe number. But these password are more and more easy 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.

iii. Special of Character

Say: Using Special character like: @ $ % & make the password extra secure and harder to guess. Nowadays, some websites require you to use a special character to to cvalidate 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

Show slide x : list of password managers

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.

2 Zoho.com https://www.zoho.com/vault/educational-content/what-is-a-password-manager.html#:~:text=A%20password%20manager%20allows%20individuals,required%20to%20remember%20multiple%20passwords.

یەکێکی تریان ئەوەیە کە ئەگەر هاکەرەکە ژیری دەستکرد (AI) بەکار بهێنێت و هەوڵ بدات هارد دیسکەکەتان بەزۆر بکاتەوە، ئەگەری شکاندنی نهێنوشەی ٥ پیتی زۆر ئاسانتر نهێنوشەی درێژ .

2. ئاڵۆزی

بڵێن: زۆربەمان، لە کاتی دروستکردنی نهێنوشەدا، زۆرجار وشەیەک و ڕەنگە ژمارەیەک بەکاردەهێنین. بەڵام ئەم نهێنوشانە بەهۆی نەرمەکاڵا و ئامرازە نوێیەکانەوە بۆ درزکردن و شکاندن ئاسانن کە لە یەک چرکەدا هەموو وشە ناسراوەکان دەپشکنن. ئەم نەرمەکاڵایانە زۆرجار AI (ژیری دەستکرد) بەکاردەهێنن. لێرەوەیە کە هەمیشە باشترە زنجیرەیەک پیتی ڕەمەکی هەبێت نەک وشەیەک.

3. تایبەتی کارەکتەری

بڵێن: پیتی تایبەت وەک: @ $ % & بەکاربهێنن و بەم جۆرە نهێنوشەکە پارێزراو و قورستر بکەن بۆ پێشبینیکردن. لە ئێستادا هەندێک ماڵپەڕ داوا دەکەن کە بۆ پشتڕاستکردنەوەی نهێنوشەکەمان کاراکتەری تایبەت بەکاربهێنین بەڵام بەداخەوە هەموویان نا.

بڵێن: خراپترین نهێنوشە کە دەتوانن بەکاری بهێنن یەک وشەیە. لەوێوە دەست پێدەکات و هاکەر دەتوانێت ئەو شتە بەکاربهێنێت کە پێی دەوترێت هێرشی فەرهەنگ بۆ درزکردنی وشە نهێنیەکانتان. هێرشی فەرهەنگ دەتوانێت کار لەسەر وشەیەک بکات. هەروەها ڕۆژی لەدایکبوون، ناو یان تەنانەت "123456789".

گەورەترین کێشە کە هەمانە ئەوەیە کە لە سەردەمی مۆدێرندا چەندین پاسۆردمان هەیە بۆ چەندین ئەکاونتی جیاواز و ئامێرەکانمان. جگە لەوەش ئەگەر زانیاری هەستیارتان هەبێت، دەتانەوێت هارد دیسک و کۆگای هەور (cloud storage) بە وشەی نهێنی جوان و بەهێزی ٣٦ پیت کۆد بکەن کە پێدەچێت بە ئاسانی وەبیری نەهێننەوە. چارەسەری ئەم کێشەیە بەکارهێنانی بەڕێوەبەری نهێنوشەیە.

ب) بەڕێوەبەری نهێنوشە

سلایدی x پیشان بدەن : لیستی بەڕێوەبەرانی نهێنوشە

بەڕێوەبەری نهێنوشە بە تاک و بازرگانییەکان ڕێگە دەدات هەموو نهێنوشەیەکی خۆیان لە یەک شوێنی سەلامەتەوە هەڵبگرن و بەڕێوەی بەرن. بەم شێوەیە، بەکارهێنەران چیتر پێویست ناکات چەندین وشەی نهێنی لەبیریان بمێنێتەوە[2]

جیاوازی نێوان بەڕێوەبەرانی وشەی نهێنی دەتوانێت نرخیاندا بێت، و هەروەها لە کوێدا وشەی نهێنیەکانتان لە ڕاستیدا هەڵدەگیرێن. بۆ نموونە بیتواردن Bitwarden وشەی نهێنیەکانتان بە شێوەیەکی تارادەیەک سەلامەت لە هەورێکدا لەسەر سێرڤەرەکانیان هەڵدەگرێت و ڕێگە بە چەند کەسێک دەدات بە ئەکاونتی جیاواز دەستیان پێی بگات. بەڵام لەوانەیە بە هەر هۆکارێک متمانەتان بە Bitwarden نەبێت و بتانەوێت داتاکانتان لە ناوخۆدا هەڵبگرن. KeyPassXC بۆ بەڕێوەبەری نهێنوشەی هەڵگیراوی ناوخۆیی نموونەیەکی باشە.

2 Zoho.com https://www.zoho.com/vault/educational-content/what-is-a-password-manager.html#:~:text=A%20password%20manager%20allows%20individuals,required%20to%20remember%20multiple%20passwords.

Having a passphrase to easily memorise 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...

Break

Part 4 : Browsing the internet confidentially

The internet was invented as a way to decentralize communication and connect one person to another's web page. It has evolved into a behemoth of a technology that

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

---

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

هەبوونی دەستەواژەیەک کە لەبیرتان بمێنێت بۆ ئەوەی بە ئاسانی بە بەرێوەبەری **نهێنوشه** دەستتان ڕابگات گرنگە، بەڵام با چاوێک لە چێنێکی تری ئاسایش بکەین کە دەتوانن جێبەجێی بکەن: 2FA

ب) ڕەسەنایەتی 2 فاکتەری

ڕەسەنایەتی دوو فاکتەری، یان 2FA، چێنێکی سەرتری پاراستنی ئاسایشی ئەکاونتە ئۆنلاینەکان بۆ دڵنیابوونە کە لە سەرووی ناوی بەکارهێنەر و نهێنوشه بەکاردێت [3].

دەتوانن بە ٢ شێواز ڕەسەنایەتی بسەلمێنن

- شتێک کە دەیزانن (وەک **نهێنوشه**)
- شتێک کە ئێوە خاوەنین یان لەبەردەستانە (بایۆمەتری)

هەواڵی خۆش ئەوەیە کە دەتوانن و پێویستە هەردووکی بەکاربهێنن. بە Factor Authentification-2 دەتوانن دڵنیا بن لەوەی کە تەنانەت ئەگەر هاکەرێک نهێنوشەکەتان بشکێنێت، ئەو چینە زیادەیەی ئاسایشتان هەیە. ئەمەش زۆرجار بەم شێوانەی خوارەوەیە :

- ئەپێک لە مۆبایلەکەتاندا کە بۆ دەستگەیشتن بەم خزمەتگوزارییە کۆدێکی کاتیدان پێدەدات (بڕوانن: Google Authenticaton)
- کلیلێکی USB وەک Yubikeys یان Nitrokeys کە کاتێک وەسل دەبێت، لە ڕێگەی دەست لێدانەوە یان تەنانەت پەنجەمۆرەکەتانەوە دەتوانن دەستتان بگات بە کۆدەکان و ڕێگەتان پێبدەدات بچینە ناو ئەکاونتەکەتانەوە.

2FA بە خێرایی بووەتە پێوەرێک لە ئاسایشی دیجیتاڵیدا. زۆربەی ئەکاونتەکانی سۆشیال میدیا لە ئێستادا ڕێگە بە 2FA دەدەن و ئەگەر دەستتان دەگات، پێویستە لەو ساتەدا کە ئەم پۆلە بەجێدەهێڵن، سیستەمی 2FA لەسەر زۆربەی ئیمەیڵ و نامە و ئەکاونتەکانی سۆشیال میدیا جێبەجێ بکەن.

ب) پاراستنی هارد دیسک و سیستەمی هەڵگرتنی هەور

جگە لە کۆدکردنی هاردەکەتان، بیر لە بەکارهێنانی هارد دیسکێکی دەرەکی بۆ سیستەمی کلاود کە پشتڕاستکراونەتەوە بکەنەوە، وەک: Google Cloud، OneDrive...

شکاندن

بەشی چوارەم : گەڕان بە ئینتەرنێتدا بە نهێنی

ئینتەرنێت وەک ڕێگەیەک بۆ لە مەرکەزییەت دەرهێنانی (decentralize) پەیوەندییەکان و وەسڵ کردنی کەسێک بە وێب پەیجی کەسێکی دیکەوە داهێنرا. ئەمە پەرەی سەندووە و بوومتە زەبەلاحێکی تێکنەلۆژیا.

پێش ئەوەی کە بە شێوەیەکی پارێزراو دەست بکەن بە گەڕان، زانیاری لەسەر ئەم خاڵانەی خوارەوە زۆر گرنگە:

---

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

- 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[4], that regulate your IPs relationship with all the other Ips that constitute the world wide web (think of it as like 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 : Using Web Browsers : what web browsers do you all use?

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

In general its good to have 2 web browsers, one that had has 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

---

4A 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)

- دابینکەری خزمەتگوزاری ئینتیرنێتییەکەتان کێیە؟
- سروشتی ناونیشانی IP ییەکەتان چییە؟ ئایا چاک کراوە یان دەگۆڕدرێت؟ ناونیشانی IP یەکەتان بۆ تۆڕی ماڵەوە یان شوێنی کارەکەتان وەکو ناسنامەکەتان وایە.
- ڕێکخستنەکانی(تەنزیماتی) دیواری ئاگرەکەتان (Firewall) چین[4]، کە پەیوەندی IPیەکەتان لەگەڵ هەموو IP یەکانی تر کە وێبی جیهانی پێکدەهێنن ڕێکدەخات (وەک سیاسەتێکی کۆنترۆڵکردنی سنوور بۆ ئەوەی کێ دێتە ژوورەوە و کێ دەردەچێت بیری لێبکەنەوە)

آ) بەکارهێنانی VPN

بپرسن: ئایا کەسێک دەتوانێت بۆمی ڕوون بکاتەوە کە VPN چییە؟

بڵێن: VPNیان Virtual Private Network کۆمپیوتەرەکەتان بە سێرڤەرێکی ترەوە دەبەستێتەوە(وەسڵ دەکات) و دواتر لەو ڕێگەیەوە دەچێتە ناو ئینتەرنێت و چالاکییەکانتان دەشارێتەوە. هەروەها هەندێک جار دەتوانێت شوێنەکەتان بشارێتەوە و ڕێگەتان پێبدات بلۆکی شوێنی جوگرافی دەور لێبدەن.

بەڵام ئاگادار بن کە VPN لە کوژانەوەی ئینتەرنێت ناتانپارێزێت، چونکە IP یەکەتان لە کاتی کوژانەوەی ئینتەرنێتدا هەر "چالاک" دەبێت کە هەوڵی دەستگەیشتن بە VPN دەدات، و ئەمەش دەتوانێت ئێوە لاواز بکات و زەربەتان لێبدات.

VPN باشەکان بریتین لە NordVPN یان Mullvad، بەڵام بەگشتی ئێوە VPNێکتان دەوێت کە ڕاپۆرتەکان تۆمار نەکات، چونکە لە بنەڕەتدا تەنیا لە دابینکەری خزمەتگوزاری ئینتەرنێتەکەتانەوە بۆ دابینکەری VPN دەیگوازێتەوە کە دواتر دەتوانێت ئەو زانیارییانە بفرۆشێت یان خراپ بەکاربێنێت.

ب) وێبگەڕەکان

بپرسن : بەکارهێنانی وێبگەڕەکان : ئێوە چ وێبگەڕێک بەکاردێنن؟

- گووگڵ کرۆم
- مۆزیلا فایەرفۆکس
- مایکرۆسۆفت ئێدج
- Brave؟ ڤیڤاڵدی؟

بەگشتی باشە کە ٢ وێبگەڕتان هەبێت، یەکێکیان کە ئەکاونتەکانی ئێوەیان هەبووە و بۆ بەکارهێنانی کاری پیشەیی یان تایبەت هاوکات کراوە(هەماهەنگ کراوە)، و یەکێکی تریان بۆ ئەوەی بە سادەیی و ئاسایی بۆ شتێک بگەڕێن. ئەمەش لەبەر ئەوەیە کە مەکینەی(ماشینی) گەڕان، مێژووی گەڕانەکەتان هەڵدەسەنگێنێ و ئەزموونی گەڕانەکەتان دەستکاری دەکەن و دەیگۆڕن.
بەگشتی مۆزیلا فایەرفۆکس و ڤیڤاڵدی وێبگەڕگەلێکی سالمن (ئەمنن). کرۆم و ئێم ئێس ئێدج لەلایەن

4 ڕێکخستنی فایەروالڵ بریتییە لە کۆمەڵێک پرۆفایل یان یاسا. ئێوە ئەم پرۆفایل یان یاسایانە بۆ دیاریکردنی مۆڵەتەکان(ئیجازەنامەکان) بۆ هەموو پەیوەندییەکان کە دێنە ژوورەوە و دەچنە دەرەوە، بۆ دەروازە تایبەتەکان لەسەر کۆمپیوتەر جێبەجێ دەکەن. (IBM.com)

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.

Part 5 : Protecting you from Phishing and malware

Phishings: "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].

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 ask 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 its 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 unpacks itself : it creates an operating system within an operating system.

---

5 Data mining is the practice of analysing large databases in order to generate new information.
6 Oxford Dictionnary
7 Oxford Dictionnary

گەشەپێدەرانی نەرمەکاڵا گەورەکان کە دەیانەوێت داتاکانتان بگرن و بە هۆکاری بازرگانی بەکاری بهێنن. دەتوانن شتە بەدەست بهێنن کە پێی دەوترێت unGoogled Chromium کە سەرچاوەیەکی کراوەیە و هەموو ئەو شتانەی گووگڵ کە لە داتا ماینینگدا دروستکراون[5] لا دەبات. هەروەها Brave هەندێک شیکاری دروستکراوی هەیە بەڵام هەندێک تایبەتمەندی ئەمنی زۆر بەهێزیشی هەیە.

وێبگەڕە تەواو ناپارێزراوەکان(نائەمن) بۆ چالاکوانانی مافی مرۆڤ بریتین لە ئۆپێرا (کە داتاکانی ڕاستەوخۆ دەچێتە سەر سێرڤەرێکی چینی) و هەروەها وێبگەڕە ناوخۆییەکان کە لەلایەن کۆمپانیاکانی ڕیکلامکردنەوە دیزاین کراون.

بەشی پێنجەم : پاراستنتان لە فیشینگ و بەرنامە زیانبەخشەکان

فیشینگس: "ساختەکاری ناردنی ئیمەیڵ یان نامەی تر کە گوایە لە کۆمپانیا بەناوبانگەکانەوە هاتبێت بە مەبەستی هاندانی تاکەکان بۆ ئاشکراکردنی زانیاری تاکەکەسی، وەک وشەی نهێنی و ژمارەی کارتی بانکی"[6].

بەرنامەی زیانبەخش: "نەرمەکاڵایەکە(بەرنامە) کە بۆ تێکدان، زیانگەیاندن، یان دەستڕاگەیشتن بە سیستەمی کۆمپیوتەر بەبێ مۆڵەت(ئیجازە) دروستکراوە"[7]

هێرشی فیشینگ زۆرجار پەیوەندی بە ئیمەیڵەوە هەیە بەڵام لە ڕاستیدا لە هەموو بوارەکانی تری پەیوەندیکردندا لەبەردەستن. بیرۆکەی فیشینگ ئەوەیە کە ئێوە بە ڕواڵەت بە نیشاندانی کەسێکی متمانەپێکراو، چەواشەکاری پێشکەش دەکەن(فریو دەدەن). لەوانەیە گوێتان لە فیشینگ بووبێت.

لەم ڕۆژانەدا، فیشینگ زۆرتر لە ڕێگەی ئیمەیڵەوە ئەنجام دەدرێت بەڵام ڕەنگە گوێتان لە ماسیگرتن بە بەکارهێنانی ئەپی پەیوەندیکردن (دۆزینەوەی هاوڕی) بووبێت. لە ڕۆژانی کۆندا فێڵبازەکان لە ڕێگەی تەلەفۆنەوە پەیوەندیان بە خەڵکەوە دەکرد. هاکەرێک کە فیشینگ بەکاردەهێنێت کەسێکە کە هەوڵی ئەندازیاری کۆمەڵایەتی دەدات و تا لە ئەندازیاری کۆمەڵایەتی باشتر بێت دەتوانێت زیانێکی خراپترتان پێبگەیەنێت.

با چاوێک لە هەندێک نامە بکەین کە لینک و پەیوەندی وایان تێدایە کە لەوانەیە فیشینگ بن :

سلایدەکان بە نموونە پیشان بدەن و بپرسن چۆن دەکرێ بناسرێنەوە.

بڵێن : بیرۆکەکە لێرەدا ئەوەیە ئەگەر بەستەرێکی وەک ئەم بدۆزیتەوە پێویستە بتوانیت ژینگەیەک دروست بکەیت کە کلیککردن لەسەری و دابەزاندنی، هەر بەرنامەیەکی زیانبەخش تێیدا ئیزولە کرێت. ئەمەش بە Sandboxing ناسراوە و لە ئاسایشی ئەلیکترۆنیدا چەمکێکی گرنگە. شێوازی کۆنی ساند بۆکسکردن تەنها هەبوونی کۆمپیوتەرێکی ئۆفلاین، کارکردن لەسەری و دڵنیابوون لەوەی کە توانایی پەیوەندیکردنی بە ئینتەرنێتەوە نییە. تا دێت دەتوانن بە دانانی Virtual Machine زۆرتر و زۆرتر sandbox بکەن.

ئامێری مەجازی وەک یەکێک لەو بووکە شووشە ڕووسییانە وایە کە خۆی دەکاتەوە : سیستەمێکی کارپێکردن لەناو سیستەمێکی کارپێکردندا دروست دەکات.

8 Data mining is the practice of analysing large databases in order to generate new information.
9 Oxford Dictionnary
10 Oxford Dictionnary

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.

Part 6 : 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 centralise 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

<show 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 look 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 en 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 organisation or even individual in order to have your email hijacked or simply to obtain information whilst posing as you. To combat against 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

لە کۆتاییدا، بە تایبەت ئەگەر لاوازن و بەردەوام کۆمەڵێک بەرنامەی زیانبەخش لە ئیمەیڵەکەتانەوە، لەو ماڵپەڕانەی کە سەردانیان دەکەن یان لە خزمەتگوزاری نامە ناردنەکەتانەوە وەردەگرن – و بەڕاستی بۆ ئاسایشی ئەلیکترۆنی بەپەرۆشن، سەیرێکی ئەو سیستەمانە بکەن کە sandboxing وەک بنەمایەک بەکاردەهێنن. نموونەیەک بریتییە لە QubesOS کە وا دەکات کە بتوانن "ژینگەگەلێک"ی جیاواز دروست بکەن کە توانایی پەیوەندیکردن لەگەڵ یەکتریان نییە.

بەشی شەشەم : دڵنیابوون لە پارێزراوی پەیوەندییەکانتان

بپرسن : بۆچی لە وڵاتێک وەک ئێران سیستەمی کورتەنامە ئەمن نییە؟

بڵێن : لە حکومەتە دیکتاتۆرییەکاندا، خزمەتگوزاری مۆبایل و دابینکەرانی خزمەتگوزاری ئینتەرنێت زۆرجار ئەو داتایانە کە لە مۆبایلەکەتانەوە دێنە ژوورەوە و دەردەچن لە ڕێگەی ئەو خزمەتگوزارییانەوە کە کەڵکیان لێوەردەگرن تەرکیز(موتەمەرکز) دەکەن، وەک کورتەنامە. هەر بۆیە بەکارهێنانی کۆدکردنی کۆتایی بە کۆتایی زۆر گرنگە.

کۆدکردنی کۆتایی بە کۆتایی یان (E2EE) شێوازێکی ئاسایشە کە چەت و نامەکانتان بە پارێزراوی دەهێڵێتەوە. ئەو بیرۆکەیە ئەوەیە کە دوو کەس یان زیاتر لە دوو کەس کلیلێکی گشتی و کلیلێکی تایبەتیان هەیە.

کلیلی گشتی بۆ هەر کەسێک کە داوای بکات لەبەردەستە و کلیلە تایبەتییەکەتان کۆدی کلیلە گشتیەکانی تر دەکاتەوە. بۆ ئەوەی باشتر لە کۆدکردنی کۆتایی بە کۆتایی تێبگەن، لێرەدا ڤیدیۆیەکی یارمەتیدەر هەیە.

<ڤیدیۆ پیشان بدەن>

بڵێن : ئێستا وادەزانم هەموتان ئیمەیل بەکاردەهێنن و لە بەرامبەر واتساپ، ئینستاگرام، سناپچەت و ئەپەکانی تری نامە ناردن کە سەلامەتترن و سەیرمان کردوون، تارادەیەک تەکنەلۆژیایەکی کۆنترە. هەر بۆیە زۆر گرنگە لەوە تێبگەن کە چ دابینکەرێکی ئیمەیل بەکاربهێنن، چ جۆرە هەڕەشەیەک هەیە و لە کوێدا بەدوای سەرچاوەی زیادەدا بگەڕێن.

ئەکاونتی ئیمەیل دۆمەینی وەک gmail.com@ بەکاردەهێنن بۆ ئەوەی ئاماژە بەوە بکەن کە کام سێرڤەر بەکاردەهێنن بۆ گواستنەوەی نامەیەک لە ڕێگەی ئینتەرنێتەوە. زۆرجار ئیمەیلی کارەکەتان، سێرڤەرەکانی کارەکەتان بەکاردەهێنێت و organisationname.com@ ی دەبێت. زۆربەی ئەکاونتەکانی ئیمەیڵ لەلایەن دابینکەری خزمەتگوزاری ئیمەیڵ وەک گووگڵ یان مایکرۆسۆفت بەڕێوەدەبرێن.

یەکێک لە هەڕەشە سەرەکییەکان جگە لە فیشینگ، بریتییە لە ساختەکردنی دۆمەین.

ساختەکردنی دۆمەین بریتییە لە هەوڵدان بۆ بەکارهێنانی دۆمەین و ناسنامەکەتان وەک ڕێکخراوەیەک یان تەنانەت تاکێک بۆ ئەوەی ئیمەیلەکەتان بدزرێت یان تەنها بۆ بەدەستهێنانی زانیاری لەکاتێکدا خۆیان وەک تۆ پیشان دەدەن. بەرەنگاربوونەوە لە بەرامبەر ساختەکردنی دۆمەین ڕاپۆرتکردنە.

هەروەها کۆدکردنی کۆتایی بە کۆتایی لە ئیمەیلدا لە کاتی ئاڵوگۆڕی زانیاری یان فایلێک کە هەستیارە، ئامرازێکی بەسوودە. دابینکەرانی ئیمەیل وەک gmail و outlook لە کۆدکردنی کۆتایی بۆ کۆتایی نایەنە دەرێ.

ecryption. For gmail though there is an extension you can install called Mailvelope that can encrypt. Email providers that use end-to-end ecryption and even have tools to allow only the recipient to decrypt a message even they do not 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 specialised use.

Part 7 : 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.

Show slide x

Say : The Pegasus scandal[8] 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 your phone, making it especially illegal. But more importantly what this shows is that our phones are very easily turned into a portable surveillance device. 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 has 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.

---

6 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.

ئەگەرچی بۆ gmail شتێک هەیە بە ناوی Mailvelope کە دەتوانن دایمەزرێنن و دەتوانێت کۆد بکات. ئەو دابینکەرانەی کە کۆدکردنی کۆتایی بە کۆتایی بەکاردێنن و تەنانەت ئامرازی وایان هەیە کە تەنیا ڕێگە بە وەرگرەکە دەدات کۆدی نامەیەک بکاتەوە و تەنانەت کلیلی گشتی ئێوەشیان نییە، بریتین لە Protonmail و Tutanota.

خاڵی لاوازیان ئەوەیە کە ئەمانە زیاتر لەگەڵ مشتەرییەکانی ئیمەیلدا کێشەی گونجانیان هەیە و ژینگەیەکی_سەرچاوەی داخراون کە بەراورد بە جیمەیل و ئاوتلۆک زۆر تازەپێگەیشتوو و نوێن، بەڵام بە دڵنیاییەوە بۆ بەکارهێنانی تایبەت شایەنی سەیرکردنن.

بەشی حەوتەم : ئاسایشی مۆبایل

پرسیارێکی خێرا بکەن کە کێ کام سیستەمی کارپێکردنی مۆبایل بەکاردەهێنێت (iOS vs Android)

بڵێن : ئێمە بە کورتی باسمان لە ئەپی نامە ناردن لە مۆبایلەکەتاندا کردووە ، بەڵام هاتنی مۆبایلە زیرەکەکان چەندین چەڵێنجی دیکەی بۆ پسپۆڕانی ئاسایشی ئەلیکترۆنی بەرهەم هێناوە. یەکێکیان ئەوەیە کە زۆر بە باشی هەموو ژیانتان ئێستا لە مۆبایلەکەتاندا دەدۆزرێتەوە، و وەک لە سەرەتای پۆلەکەدا وردی باسمان کرد...

سلایدی x پیشان بدەن

بڵێن : ڕسوایی Pegasus[8] دەریخست کە تەنانەت حکومەتە دیموکراتیکەکانیش ئامادەن سیخوڕی لە هاوڵاتیان بکەن کە بە بەکارهێنانی ئەو شێوازانەی فیشینگ کە لە سەرەوە بینیمان (لە ڕێگەی نامەیەکی کورتەوە) ئەو کارەیان کردووە. ڕەنگە زۆرێک لە ئێوە پێشتر پێتان وابووبێت کە NSA و GCHQ و کۆمپانیا جۆراوجۆرەکانی دیکەی سیگنالّ ئینتلیجنس(Signals Intelligence) پێشتر سیخوڕیان لێتان کردبێ، بەڵام ڕاستییەکە ئەوەیە کە پێش پێگاسۆس، ئەم گروپانە تەنیا دەیانتوانی پەیوەندییەکانی نێوان خۆتان و لایەنی سێیەم بخوێننەوە. جیهانی دوای پێگاسۆس ترسناکە چونکە ئێستا دەتوانن چاودێری تەواوی مۆبایلەکەتان بکەن و بەم شێوەیە هەر هاکەرێکی باش بە ئامرازێک دەتوانێت بۆ ئەوەی لاواز بن زانیاری تەواو لەسەرتان بەدەست بێنێت.

ئازادکردنی بەرنامە زیانبەخشەکان وەک Pegasus دەستڕاگەیشتن بە هەموو مۆبایلەکەتان بۆ هاکەرەکان دابین دەکات و ئاسانی دەکاتەوە، ئەمەش وایکردووە کە بە تایبەتی نایاسایی بێت. بەڵام لەوەش گرنگتر ئەوەیە کە مۆبایلەکانمان زۆر بە ئاسانی دەکرێنە ئامێرێکی چاودێری پۆرتەبل(واتە شتێک کە هەڵدەگیرێت و بە ئاسانی ئەملاوئەولای پێدەکرێت) وە دەتوانن ئەو ڕاستییە زیاد بکەن کە گووگڵ و ئەپڵ و خزمەتگوزارییەکانی تری مۆبایل بە هۆکاری بازرگانی داتاکانتان لێ کۆدەکەنەوە، کە ئەگەر ئەم داتایانە بکەونە دەستی کەسی نادروست دواتر دەتوانرێت لە دژی ئێوە بەکاربهێندرێت.

خۆشبەختانە کۆمەڵێک بەدیل هەیە بۆ ئەوانەی کە نایانەوێت بە بەکارهێنانی مۆبایل لاواز بن. Graphene OS و Lineage OS نموونەی ئەو شتانەن کە ئێمە پێی دەڵێین فورک کۆدی ئەندرۆید، کە هەموو خزمەتگوزارییەکانی پەیوەندیدار بە گووگڵی سڕیوەتەوە. هەروەها دەتوانن سەیری سیستەمی کارپێکردنی مۆبایلەکان بکەن کە دەتوانن بە شێوەیەکی کاریگەر ساند بۆکسینگ بەکاربێنن بۆ ئەوەی دڵنیا بن لەوەی کە هەر ئەپێک کە دایدەمەزرێنن سیخوڕی لەسەر کەسانی تر ناکات.

6 کە ئەمەش فەزیحەی ئەو تۆمەتانەیە کە دەڵێن نەرمەکاڵای سیخوڕی ناسراو بە پێگاسۆس ڕەنگە بۆ چاودێریکردنی ڕۆژنامەنووسان و چالاکوانان و ڕەنگە سەرکردە سیاسییەکانی ئیسپانیایش بەکار هاتبێت.

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-domianted digital environment, your best bet a s a human rights activist is to use these tools as sparingly as possible or with very specialised software.

Part 8 : 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 your doing is essential too. There exists 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 works, 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 learn how to set up your own sever

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

بەڵام ئاگاداربن بەگشتی بۆ سیخوڕیکردن لەسەرتان، مۆبایلەکەتان ئامرازێکی تەواو و گونجاوە. لە درایڤەری ڕەقەکاڵاکانەوە تا ئەپی یاریکردن کە دایدەبەزێنن، زۆربەی تەکنەلۆژیای مۆبایلەکەتان سەرچاوەی داخراوە: ئێوە نازانن کە گەشەپێدەر چ کۆدێکی خستوتە سەر مۆبایلەکەتان. لەگەڵ پەرەسەندنمان بۆ ژینگەیەکی دیجیتاڵی کە زیاتر مۆبایلە زیرەکەکان و تابلێتەکان زاڵن، وەک چالاکوانێکی مافی مرۆڤ، باشترین مەرج ئەوەیە کە تا دەتوانن ئەم ئامرازانە بە کەمی یان بە نەرمەکاڵایەکی زۆر تایبەت و تەخەسوسی بەکاربێنن.

بەشی حەوتەم : چەند ئامۆژگارییەکی کۆتایی و پرسیارە بەردەوامەکان

بڵێن : با بچینە سەر هەندێک پرسیاری زۆر باو کە ڕەنگە هەندێکتان بتوانن یارمەتیم بدەن وەڵامیان بدەمەوە، و پاشان وۆرک شۆپێکی بچووک ئەنجام بدەین کە لەودا ئەوە ئێوەن کە لە من دەپرسن.

بپرسن: ئایا پێویستە دژەڤایرۆسێک دابنێم؟ ئەگەر بەڵێ کامیان؟

بڵێن: لە ئێستادا زۆرجار دژەڤایرۆسەکان لەناو سیستەمی کارپێکردنەکاندا دروست دەکرێن. ئەو ڕۆژانە ڕۆیشتن کە ویندۆز پشتی بە دابینکەرانی دژەڤایرۆسی لایەنی سێیەم دەبەست بۆ ئەوەی زۆرێک لە کارە قورسەکان لە دژی بەرنامە زیانبەخشەکان ئەنجام بدەن. ئەپڵ و لینوکس بەرامبەر بە بەرنامە زیانبەخشەکان زۆر بەهێزن، دووەمیان بەهۆی فەلسەفەی سەرچاوە کراوەی خۆیەوەیە. Open Source remember لەبیرتان بێت سەرچاوە کراوەی واتە کۆدەکە کراوەیە بۆ هەموو کەسێک و بەزۆری لەلایەن کۆدکەرانی ترەوە بۆ پشترِاستکردنەوەی یەکپارچەییەکەی وردبینی دەکرێت.

سەرەڕای ئەوەش ئەگەر بینیتان دژەڤایرۆسێک دامەزراوە یان بتانەوێت یەکێکیان بکڕن، دژەڤایرۆسەکان بەگشتی ئامرازی شیکاری داتان کە چاودێری دەکەن لە کوێ و چۆن کۆمپیوتەرەکەتان سەرچاوە بەکاردێنێت، چ فایلێک پێدەچێت تێکچووبێت یان بە شێوەیەکی تر گوماناوی بێت و هەروەها دەتوانێت یارمەتیتان بدات لە بەهێزکردنی دیواری ئاگرەکەتان - ئەو دیوارەی کە ڕێگری دەکات لەوەی ئەکتەرە خراپەکان بچنە ژووروەوەی ئادرەسی تۆر/ئایپیەکەتان. دژەڤایرۆسێکی باش بریتییە لە Bitdefender، بەڵام ئەگەر فێربوون چۆن ساندبۆکس بکەن و سیاسەتی دژەڤایرۆسی عەقڵی ساغ بەکاربێنن پێویستتان پێی نییە.

بپرسن: ئایا بەڕاستی ئەپڵ لە ویندۆز سەلامەتترە(ئەمنترە)؟

بڵێن: وایە، بەڵام هێشتا لە ئەگەری لاوازیی و زەربەدایە. هەڵبژاردنی سیستەمی کارپێکردنی گونجاو بۆ کارێکی گونجاو کە دەیکەن زۆر گرنگە. زۆر سیستەمی کارپێکردنی لینوکس بەخۆڕایی هەن کە بە بەراورد بە پێشکەشکردنی ئەپڵ و مایکرۆسۆفت زۆر بە سەلامەتتر و پارێزراوتر دادەنرێت، بەڵام ڕەنگە کەمێک شارەزایی تەکنیکی زیاتریان پێویست بێت. بەڵام ئەگەر بڕیارە دەربارەی چۆنیەتی کارکردنی سیستەمی کارپێکردنی لینوکس بچنە ناو فێربوونی ئاسایشی ئەلیکترۆنییەوە، هاککردنی ئەخلاقی لە ڕێگەی کالی لینوکس و تەنیا جیاوازییە سەرەکییەکانی سیستەمی کارپێکردن بۆ سێرڤەر و هەروەها بۆ بەکارهێنانی تاکەکەسی زۆر گرنگە.

بپرسن : لە کوێوە دەست پێ بکەم ئەگەر بمەوێت زیاتر بچمە ناو ئاسایشی ئەلیکترۆنییەوە؟

بڵێن : وەک پێشتر وتمان زۆر دۆمەین هەیە کە دەتوانن لە بواری ئاسایشی ئەلیکترۆنیدا دابینێن. سەرەتایەکی باش، فێربوونی بنەماکانی بەرنامەسازی ڕەقەکاڵا و نەرمەکاڵایە بۆ ئەوەی لانیکەم لە پەیوەندی نێوان ئەو دووانەدا خوێندەوار بن و دواتر فێر بن چۆن سێرڤەری خۆتان دابنێن.

بپرسن : چۆن بزانم کۆمپیوتەر یان مۆبایلەکەم هاک کراوە؟

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

TIP

- 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 :

- For specific accounts, you can check if you have been subject to a data leak or hack through this website :

- For email or your personal website in particular, you can check if your domain has been spoofed through looking at the domain :

Ask: What are some resources if I need help as a human rights activist?

TIP

- 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.

بڵێن : وەک پێشتر وتمان، زۆرجار دەرک بەوە ناکەن کە هاک کراون، پێش ئەوەی زۆر درەنگ بێت، چونکە هاکەرەکان مەیلیان هەیە لە کۆتایی پشتەوەی سیستەمی کارپێکردنەکەتاندا کاربکەن (دەستگەیشتن بە فایلەکان بەبێ ئەوەی بزانن).

سەرنج

- بۆ کۆمپیوتەر دەتوانن فایلە گوماناوییەکان بە بەکارهێنانی ئەم ماڵپەڕانەی خوارەوە بپشکنن :
- بۆ مۆبایلەکان، ئێستا چەند ئامرازێکی نایاب هەیە بۆ ئەوەی بزانن ئایا لە ژێر کاریگەری سیخوڕی یان بەرنامەی زیانبەخش هەن یا نە :

- بۆ ئەکاونتی تایبەت دەتوانن لە ڕێگەی ئەم ماڵپەڕەوە بزانن کە ئایا تووشی دزەکردنی(لیک) داتا یان هاک بوون :

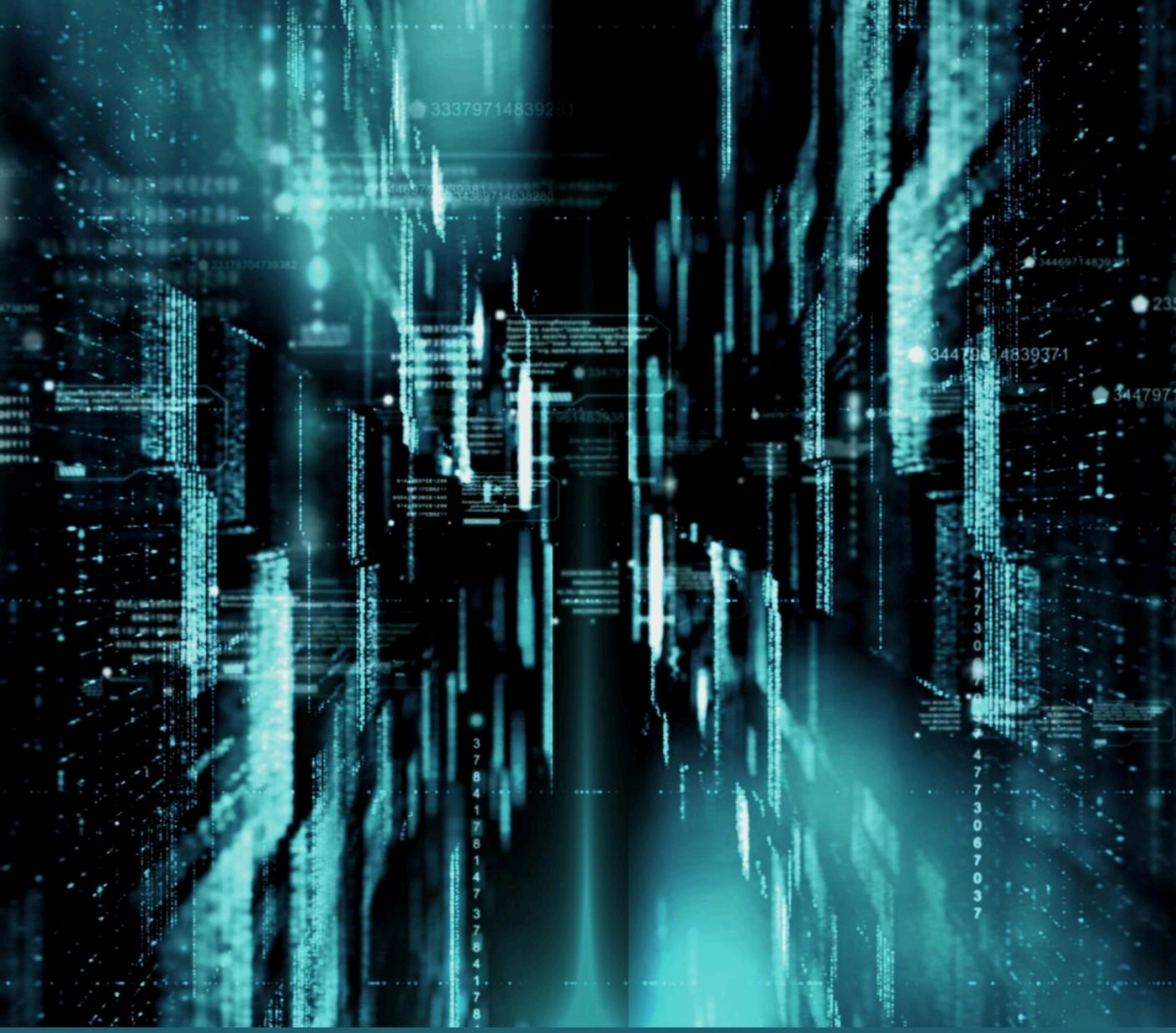
- بۆ ئیمەیڵ یان ماڵپەڕی تایبەتی خۆتان بە تایبەتی دەتوانن لە ڕێگەی سەیرکردنی دۆمەینەکەوە بزانن کە ئایا دۆمەینەکەتان ساختە کراوە یان نا :

بپرسن: ئەگەر وەک چالاکوانێکی مافی مرۆڤ پێویستم بە یارمەتی هەبێت چ سەرچاوەگەلێک هەن ؟

سەرنج

- AccessNow
- ڕێکخراوی لێبوردن
- سەنتەری خۆڕاگری دیجیتاڵی
- UNPO

پاشان بە پشتبەستن بە ئامادەبووان و ئەوەی چ ئامێرێکیان لەبەردەستدایە، سەرپەرشتی وۆرک شۆپێک بکەن کە کەیسی تاکەکەسی زیاتری تێدابێت.



DIGITAL SECURITY TRAINING PACK

2023

♦ - It♦ UNREPRESENTED

- NATIONS & PEOPLES