Hello everyone and welcome to the second lesson of the fourth week of the course on “Online harassment: strategies for journalists’ defense.”

During the last session, I talked about how we can secure our accounts to prevent harassers from having access to them and compromising our security and privacy.

For this lesson, we will dive deeper into safe browsing and safe communications. All our life is currently happening online. It is true that the digital transformation started a few years ago, but with the Covid-19 pandemic, our digital presence and activity increased remarkably, and we’ve witnessed a drastic and fast change. Now, all our meetings, conferences, professional or personal communications are strictly happening online.

With this digital transformation, the digital risks became bigger and more prominent.

Let’s start talking about how to safely browse the internet. During the previous lesson, I mentioned that one of the tips to secure our accounts was to clear our browsing history. Why is that?

Probably by now, after years of using the internet, whether through browsers or social media platforms, the internet already knows a lot about us. We should keep in mind that whatever the internet knows about us becomes accessible to harassers.

Therefore, to protect your privacy, it is recommended to use a VPN.

What’s a VPN?

A VPN can be compared to a secure tunnel between your PC and the destination you want to visit on the internet which is the website. When your PC is connected to a VPN, it masks your actual location, which is discoverable through your IP address, and gives you a virtual location from which you can browse the internet. This virtual location or the VPN server is typically in another country, for example, USA, The United Kingdom, Sweden, France, etc.

So, whenever you are browsing the internet, your web traffic passes through the VPN server, and for the websites you're visiting, you will look like you are browsing from the server’s geographical location, not your PC’s actual location.

So, this is why a VPN is used to access banned websites in your country. When a website is banned by the government, technically, this means that the government denied access to the site to all those located in a certain geographical area or country. When the VPN masks your actual location, you will be able to access the website because, virtually, you will be accessing it from a different location. This is why journalists and activists in repressive countries use VPN technology to communicate securely.

VPNs also protect your privacy when using public WiFis.

So let’s say you were at a coffee shop and are using the coffee shop’s public WiFi network, that you do not know if it is secure or not. Any person connected to the same network and without you knowing, will be able to steal your files and data sent from your laptop or mobile device. Therefore, while using a VPN, your internet traffic will be encrypted. That means nobody, not even the owner of the free Wi-Fi network, can have access to your data.

The downside of VPNs is that free VPNs offer limited features. However, one of the tools that are recommended to mask your identity online is ToR (The Onion Router).

Let’s watch this video that introduces what ToR is:

And now, after learning about VPNs and how to browse the internet safely, let’s talk about the communication applications that we use on a daily basis.

As I said in the beginning of the video, our whole lives are currently happening online. That means, the most used way of communication with colleagues, friends and families are mobile chatting apps.

How do we know if an app provides secure communication or not?

The key is to know whether the app we are using provides end-to-end encryption to our messages. What does end-to-end encryption mean?

End-to-end encryption is a method of secure communication that prevents third-parties from accessing data while it's transferred from one end system or device to another.
In end-to-end encryption, the data is encrypted on the sender's system or device and only the recipient is able to decrypt it. Nobody in between, be they an Internet service provider, application service provider or hacker, can read it or tamper with it.

So, why using an encrypted messaging app?

Using an encrypted messaging app ensures only those with whom you are exchanging messages can actually decipher them, but not every messaging app contains this useful feature. If you want to protect the secrecy of your chats, you need to use a messaging app with powerful encryption software designed to prevent third-parties from invading your privacy.

While there are quite a number of good encrypted apps, many have flaws associated with their operations, their owners, or both.

Let’s go through three of the most popular messaging apps that are being used worldwide which are Signal, Whatsapp and Telegram. For every app, I will be listing the security features the app provides, as well as its security risks or flaws.

Let’s start with Signal. This app is considered to be one of the most secure messaging apps available.

1- Signal offers end-to-end encryption which means that messages sent via the Signal app can only be viewed by the sender and receiver. Not even the company behind the app can decrypt the messages. In addition to instant messages, you can also make voice calls, group messages, and encrypted video calls.
2- Signal is an open source: it has an open source code that can be viewed by anyone. This kind of transparency allows for routine auditing.
3- Signal offers the feature of Disappearing messages: for extra security, Signal allows you to make messages “disappear” after a certain amount of time that you can set.
4- Signal also allows you to set a password to access the app for extra security.

The best thing about Signal is that there are virtually no security risks detected so far.

Whatsapp

1- Whatsapp also offers end-to-end encryption of messages.

2- WhatsApp also has a “Verify Security Code” screen in the contact info screen that allows you to confirm that your calls and messages are end-to-end encrypted.

3- It offers the Two-step verification feature as an optional feature
4- Whatsapp messages are not stored, which means that your messages are only kept on the WhatsApp server for the period after you send them and before they are delivered to the receiver.

The security risk of Whatsapp is that the backups are not encrypted, especially for Android users who backup their data on Google Drive.
However, you can always turn off the data backup feature for more security.

And now, Telegram:

1- Telegram also offers end-to-end encryption of the messages
2- A Passcode lock
3- And a two-step verification feature
4- Message can self-destruct which is a feature available for secret chats only. Also, if your account has been inactive for a certain amount of time it will automatically self-destruct.
5- And offers a Remote logout feature which offers the ability to log out of other sessions from the current device you’re using.

The security risks of telegram are:

First of all, the End-to-end encryption isn’t default.

You must manually enable Telegram’s “Secret Chat” feature, otherwise chats are only encrypted between your device and Telegram’s server.

And second, If you don’t enable the Secret Chat feature, then your chat data is saved on Telegram’s servers.

Thank you for watching and listening to this lesson. I hope that you will take part in our discussion about this lesson in the discussion forum. In the next video, I will be talking about Online and offline reporting systems and what can be done to counter online harassment.