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

My name is Myra Abdallah, I’m a journalist and trainer on gender and security for journalists, currently the Arab region communications manager at WAN-IFRA and the Head of Media department at the Arab foundation for Freedoms and Equality, I am based in Beirut and I will be your lecturer this week.

For the past 3 weeks, the course covered what online harassment is and coping strategies for dealing with online harassment; privacy and how to better protect your online privacy; and trolls and their strategies, and what are the techniques for documenting abuse.

During this week, we will be addressing how to counter online harassment and be safe online, through learning the different steps and tools of digital security.

In general, harassers do not only threaten our privacy and well-being, they can also attempt to compromise our security through, for example, hacking our accounts to be able to access our data.

Therefore, it is very important to know how to secure our accounts to prevent harassers from having any access to them.

In this video, I will talk about the different ways and tools that we can use to protect our accounts.

First and foremost, we should use the first tool we have access to that is the most important gatekeeper of our accounts: passwords.

We should always use passwords, even when they are optional, and not just any password. Passwords should be long, strong, and unpredictable.

Passwords should be 18 characters and more;

Always use capital letters, numbers and special characters such as the dollar or euro sign, hashtags, exclamation mark, etc. Avoid predictable dictionary words.

Also, you should use a different password for different accounts. That way, if a hacker was able to get the username and password you use for one of your accounts, having different passwords for different accounts will prevent this data breach from having a domino effect across all you accounts.

However, it might be sometimes difficult to remember all the long and complicated passwords we set. This is why it is recommended to use a password manager. There are many good password managers available for free. When you use a password manager, the only password you need to remember is the master password that locks the password manager itself.

You should keep in mind that most people who try to hack into your account are probably people who know you personally, or who have watched you long enough to know details about you, especially if you share personal information on social media. Therefore, you should avoid using any personal information such as:

- Date of birth
- First or last name
- Pet’s name
- Favorite song

- Partner’s name
- Phone number

Second, you should activate the two-step authentication feature whenever it is available. Two-factor authentication means you need to pass another layer of authentication, not just a username and password, to get into your accounts.

Two-factor authentication verifies your identity using at least two different forms of authentication the first one is the password you enter, and the second one could be either your fingerprint or facial recognition, or your mobile phone. With two-factor authentication enabled, the password alone is useless.

Here is for example, where you can activate this feature on Facebook.

And on Whatsapp.

The third tip, which is also a very important one, is to use an antivirus.

Antiviruses protect against all types of malicious softwares. There are many programs that are used to attack your device and breach your security. For example, Ransomware encrypts your files and demands payment to restore them. Trojan horse programs seem like valid programs, but in fact they are designed to steal your private information. And there are many more types of malicious softwares.

An effective antivirus protects against them.

That said, don't reply on the built-in antiviruses that usually come with your software. It is important to install a third party antivirus, and there are a few good ones available for free.

You should also remember to update the antivirus whenever there is an update available;

if you are using a paid antivirus, remember to renew it every year, or set it on auto-renewal mode.

Tip number 4: Clear your cache

Never underestimate how much your browser's cache knows about you. Saved cookies, saved searches, and Web history could lead the hacker to many personal information such as a home address, family information, and other personal data. To better protect that information, be sure to delete browser cookies and clear your browser history on a regular basis.

Tip number 5: Turn Off the save passwords feature in browsers

First of all, because saving your passwords to your browser can put your accounts at risk either if one of your accounts was hacked, and the hacker will have access to all your other accounts to which passwords are saved in the browser, or if your device was stolen, the person who has access to your device can also have access to your accounts.

We go back here to the importance of using a password manager to keep passwords in a safe place, and also to avoid spending a lot of time typing passwords. In addition, keeping your passwords in a single, central password manager lets you use them across all browsers and devices.

And the final tip of this session would be to avoid using fingerprints or facial recognition instead of a password. As journalists, we might sometimes find ourselves in situations where our security, our physical security, not only the digital one, compromised. Having only a fingerprint or facial recognition instead of a password can put our digital security at risk if our physical security was compromised. For example, if we were detained, detainers can access our devices by forcibly pressing our finger to the mobile phone for it to read our fingerprint. And once this is done, all our data will be breached.

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 safe browsing and safe online communications.