## Learning how to better protect yourself.

Hi, thank you for joining me for this lesson. During the last lesson, we looked at

- How the internet works.
- What online privacy is?
- What private data can be collected when we are online as well as how sites and apps can track you.

In this lesson, we will learn how to better protect yourself online.

As I mentioned in the previous lesson most of the personal information online about you is unwittingly shared by family, friends and sometimes, even you!

It is this data that can be used to harass and target you.

To better protect yourself, you must first understand who wants your personal information.

Hackers and criminals may want your personal information to steal your identity, to target phishing attacks and extortion, to break into accounts containing payment information.

In the case of state actors and their agents, the information may be used to track you and your family and may lead to exposure of your sources and any sensitive information you may have.

Online harassers will often look you up online to see what personal information is available about you in the public domain.

This information is then used to harass and intimidate you with the aim of causing you harm which could happen by sharing your home location for example which could lead to people coming to your house,

shaming you by bringing sharing unflattering or personal images and videos about you,

discrediting your work and opinions or views as a journalist or driving you offline by getting their followers and others to do all the things I have mentioned above relentlessly until you decide to get offline.

This kind of behaviour is called Trolling and Ela Stapley will talk more about this topic in week three.

In some instances, online harassment escalates to off-line physical attacks and even killings.

The tactics used, and personal information sought may differ based on why a person or group is targeting you. Therefore, before you start working on a story, it is important to think about the groups of people who could attack you online as a result of publishing a story. Take steps to secure your data and your accounts.

Identity impersonation attacks happen when the abuser assumes your identity. This happens when you have a weak identity on social networking sites.

The more personal data about you available in public, the easier it is for identity theft and impersonation attacks.

So where are they getting your personal information from?

As mentioned in the first lesson Some personal data is stored in public databases. This would include voter registration data, your address and date of birth.

Money lending apps have also been flagged as a potential risk to your online privacy.

These apps have access to a lot of your personal financial records which can be sold to Third Parties. Your data is also vulnerable if these apps are hacked.

When you share professional work, your stories and media appearances on your social media profiles where you also share personal photos of your family and friends, you allow bad actors access to information about your location, your family that allows them to impersonate you easily.

This is what happened to Erin Barnes, a publicist and writer. She discovered that a bot sold by a company had used not only her name,her profile photo but also a background photograph of her husband and young daughter.

You can find out more about identity impersonation attacks in the list of additional reading resources.

One way to ensure that your private data is more secure is to make separate accounts for your work life and your personal life.

Keeping data separate means that you are spreading the risk of a person finding out details about your life from one single account.

It’s also a good idea to know what content is in your social media and email accounts and understand how that information could be used against you in the case that the account is breached.

Social media accounts hold a great deal of personal data, including private messages with family and friends, financial and health data, as well as photos and documents.

This is information that online abusers will look to circulate on the Internet with the intent of damaging your reputation or to intimidate and harass you and your family.

You should decide what information you want to allow your online community to have by changing your privacy settings.

Your network of friends including your family can agree to a common approach—not sharing any information about you and you reciprocate by note sharing any information they would not want to be shared in public.

Online abusers may work in groups like companies that create and sell fake accounts to look for your personal data online.

Fake or parody accounts can be used to spread misinformation by making it seem more credible coming from a journalist.

This is what happened to a journalist with The Indian Express who had an account created with his name and photos that was sending messages to people.

For other journalists such as South African Ferial Haferjee, who when reporting on the Gupta Leaks was harassed online by fake accounts some which were accounts that impersonated business people and tried to discredit the investigation she had done on state capture by The Gupta Family.

Accounts like these in India have been shown to be used to sell fake followers and likes to people looking to grow the appearance of their online popularity.

Some “bot farms” as they are known, have been deployed in systematic information warfare campaigns by governments.

In this investigation by Facebook and Twitter after a tip from an internet security firm, an Iranian- based social media scheme impersonated reporters, politicians and others to sway public opinion and promote Iranian political interests.

The Information available on journalists' social media accounts or on the accounts of family members and friends may not do much harm as individual pieces,

But when grouped together it can give a detailed overview of your location, the circles you move in, your habits, your likes and dislikes, political choices and much more.
Details like your location can be used to harass by Doxxing you.

Doxxing is a tactic used by online harassers to intimidate Journalists. Doxxing happens when personal information such as your phone number and email address are shared online without your consent with the intent to harm and harass you.

Ela Stapley will go into Doxxing and other strategies that trolls use to intimidate and harass journalists next week.

While you might think that there is no way to keep your data private, there are some simple things that you can do to reduce your digital footprint and better protect yourself, your family and your sources.

One of the things that you can do is before you start working on a story try and understand the groups of who could attack you online as a result of you publishing a story.

Another key point is to practice digital hygiene.

To understand how much information there may be about you, a great place to start is to search for your name on search engines.

What comes up, what photos of you exist? What platforms are you on?

Review photos, videos as well as news sections and write down any content that you may want to be taken down and make a note of where this content is stored online.

You can also check if your email accounts have been compromised in a data breach on Have I been Pawn'd. If it has you can take the necessary steps to secure your accounts.

Once you know what information is available about you in the public domain you can take steps to control and remove it.

If the content you want to remove is published on a website that you control, such as your social media, then you can simply delete the information from the site.

If the information is on sites controlled by family or friends then you can reach out to them and ask them to remove this information for you.

However, the information contained on third party sites, such as public databases or blogs, may be complicated to remove.

In some cases, there may be a formal procedure that you can follow in order to ask for the information to be deleted. In other cases, you may be relying on the goodwill of the owner of the site to remove that data for you.

Different countries have different laws and legislation around personal data in the public domain.

You may not be able to remove certain pieces of information about you online simply because it would be illegal to do so.
It can take time to remove information from the Internet so it is important to start managing your online profile as soon as you can.
You can set up Google alerts for your name. This service will let you know when your name is mentioned on the internet and you can take steps to get content that puts you at risk taken down.
This planner allows you to carry out an audit of your digital footprint so that you can get started on protecting yourself.

And don't worry in the last module Myra Abdallah will take you in-depth on this and more steps that you can take to protect your privacy online.

Remember that monitoring yourself online is not a one-time thing.

You have to regularly check to see whether the content has changed or new content about you has come online.

Schedule regular reminders in your calendar that will help you to remember to check for any changes on your online platforms. Thank you for watching and listening to this lesson. Remember to go through the additional videos I have shared as well as the reading material.

I hope that you will take part in our discussion about this lesson in the discussion forum and share your thoughts and tips on what you have done to protect your online privacy.

See you all in the next lesson where we will talk about how to talk to your friends and colleagues about online privacy.