Module 2: How to talk about online privacy with friends family and colleagues.

[00:00:00] Hi, welcome to the third and final lesson in the understanding online privacy module. In the last lesson, we looked at how to protect your personal data based on the information you share on your social media profiles. However, even if you take steps to protect yourself, you are not the only one who has or shares information about yourself. Your friends, your family, your sources also share a lot of information about you. Online abusers can target your friends and family if they are unable to find information about you online.

[00:00:39] Your online privacy depends as much on your own digital hygiene as the data habits of your friends and family. Attackers are most likely to look at the social media accounts of family and friends to corroborate information about you, or to find personal information on your family that they can use to harass or intimidate them. In this lesson, we will be looking at how to talk to your friends, your family, your colleagues about online privacy.

[00:01:11] Family members and friends may not be aware of how much personal information exists about them online or how people could use their accounts to access information on you. They may also unknowingly give access to information about you without your consent. For example, if a family member installs an app and accepts to grant permission to the app to access their content, this can give backdoor access to your details. Speaking with family members about online privacy and the risks around sharing certain content can better help protect them and you from online abusers.

[00:02:01] And yet, even though they may understand what online privacy is, why it is important, the big challenge is how to make them take this issue seriously. Studies have shown that people's concern about privacy do not necessarily reflect the privacy management choices they make. This is called the privacy paradox.

[00:02:28] Before you talk to your family and colleagues about online privacy and its importance, it is important to understand the barriers to people making changes to their behavior online to better protect them as well as your own online privacy.

[00:02:47] It has been estimated that nearly 40 percent of Facebook content is shared with the default settings, which are, to say the least, rather unsafe. One of the reasons for the privacy paradox is third party bias, which suggests that even when people perceive potential risks when using social media, they sometimes somehow believe that those risks do not apply to themselves, just to others. Another more obvious explanation is a simple risk reward assessment. Most people would prefer to feel safe and protected when online, but the perceived benefits of using free sites and disclosing personal information far outweigh the perceived risks. Remember, if a service is free, then you are likely the product.

[00:03:49] Having understood the privacy paradox when starting to talk to your family, it is important to remember that not all family members will understand the technology and how it can be used against them. They may also not understand why attackers would be interested in obtaining their personal information in order to attack both you and them. I will share some useful tips that were created by IWMF with invaluable insights from Pan America.

[00:04:21] Your first step is to identify your goal as you prepared to speak to others. Do you want to let somebody know what is happening? Are you asking for help? Do you need to warn them that they may also become a target of abuse? Understanding what you want to achieve can make the conversation easier for you and them.

[00:04:44] You also need to prepare for the conversation. It can be painful and difficult to discuss online abuse. Do you want to let someone know what is happening? Are you asking for help? Do you need to warn them that they may also become a target of abuse? Understanding what you want to achieve can make the conversation easier for you and them. You also need to prepare for the conversation. It can be painful and difficult to discuss online abuse.

[00:05:16] Consider preparing what you're comfortable saying in advance and bring documentation of the abuse. This could be something that has happened to you or another journalist. Then explain why you use the internet. Relatives may not understand that you need to have an online presence to do your work. Explain how and why the internet and social media are crucial for your work as a journalist. It is also important to think about tech. How do you explain how tracking happens online? This could mean explaining things like DM's, doxxing, hacking and others. It helps to use simple language and a clean tech jargon.

[00:06:10] Don't forget to ask for support. You may find that people really want to provide support, but they don't know how. Let them know what you would find helpful, such as helping you monitor your mentions, documenting abuse, reporting harrasses, and whatever other support you might need. Remember to keep calm. If the conversation isn't going well, just remember that online abuse is real, and it's not your fault. You may need to turn to someone else for support or revisit the conversation at another time. If you're concerned about a family member's safety, help them understand the context of online abuse and provide them with practical support so they feel more in control of the situation. And lastly, be prepared to help. If you feel that family members need to secure the accounts for their safety, keep in mind that they may not know how to do that. Be prepared to walk them through the basics in person or over the phone. Many family members are likely to have an online presence, but are unaware of who can see their information and how it can be used against them, and through them, you. They may also struggle with technology and how to restrict access to their online content.

[00:07:41] You can use the following digital safety tips in order to help them be secure online. Look for your relatives online. Research what information is available about your relatives online. Once you have an idea what information is online, then you can help your family, colleagues or friends try and remove it and secure their accounts. Get their information removed from online sites. Attackers will use people finder sites to look you up as well as your relatives. In countries where this is possible, get a family subscription to a service that will remove your and their personal data from these sites. Talk about social media privacy. Your family may be unaware that the information they share on social media is not restricted and that people outside their family as well as their friends can have access to this data. Explain to family members about the difference between public facing and private accounts, social media settings, and what data is best kept private and why. Tighten safety and privacy on social media. Different social media accounts have different security and privacy settings, which can be confusing to navigate. Walk with family members to help them tighten the settings on the accounts to protect personal information. Encourage them to make their accounts private when possible. It is important to protect your mental health even as you talk to your family and colleagues. You may find that family members do not understand your concerns or may not want to remove their data from the internet.

[00:09:37] You can do the following things to help manage the conversation if it becomes difficult. Step away from the situation if the conversation becomes heated. Don't panic. You can always restart the conversation at a later date. Consider your options. Is there an ally in your family who can help you speak with others who may not understand your position? Know that it's not your fault. Online harassers do not need any reasons to target you beyond them not agreeing with you or wanting to discredit you. Agree with family and friends what information they can share about you, and what you can share about them. Seek their consent before you share out any personal information and insist they respect your privacy in a similar manner, and as much as you can be able to protect yourself online, it is important to remember that securing your friends and family's private information assures that you can manage exposure.

[00:10:49] As a journalist, criminals and hackers who want to reach you might target family and friends for online abuse and harassment. Here are a few things you can do to help them navigate the situation and secure their information. Assess the physical danger. Is your family concerned about their physical safety? Discuss whether they need to relocate temporarily, such as to a friend's home or a hotel, or maybe even install a security system. Turn social media accounts to private. All platforms allow you to tighten privacy and security settings, and some even enable you to go completely private. This will make it more difficult for abusive trolls to find personal information or make contact. Going completely private can be temporary. Check your security settings. Turn on two-step verification and ensure passwords are long and unique. Monitor the situation. Watch to see if the harassment increases, and when necessary, record the incidents and report them to the authorities. Myra Abdallah will cover this and more tips and skills on how to protect your accounts and communications in the final module of this course.

[00:12:18] Thank you for joining us this week as we learned what online privacy is, what information we should or should not share online, who would want your information, and what we need to know to protect ourselves while we are online. Remember, just as good personal hygiene is important for your health and well-being, understanding what digital hygiene is can protect you, your family, your friends, your sources from online abuses and harasses.

[00:12:53] Next week, Ela Stapley will be looking at the different kinds of online attacks, who is behind them, how they do it, how to identify such attacks, and how to create support around such attacks.

[00:13:07] Again, thank you for joining us this week, and I'm looking forward to you joining us next week.