


CYBEREQUAL

CYBER VIOLENCE AGAINST WOMEN & GIRLS (CVAWG)

Doxxing

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

CVAWG EXAMPLE

CYBEREQUAL

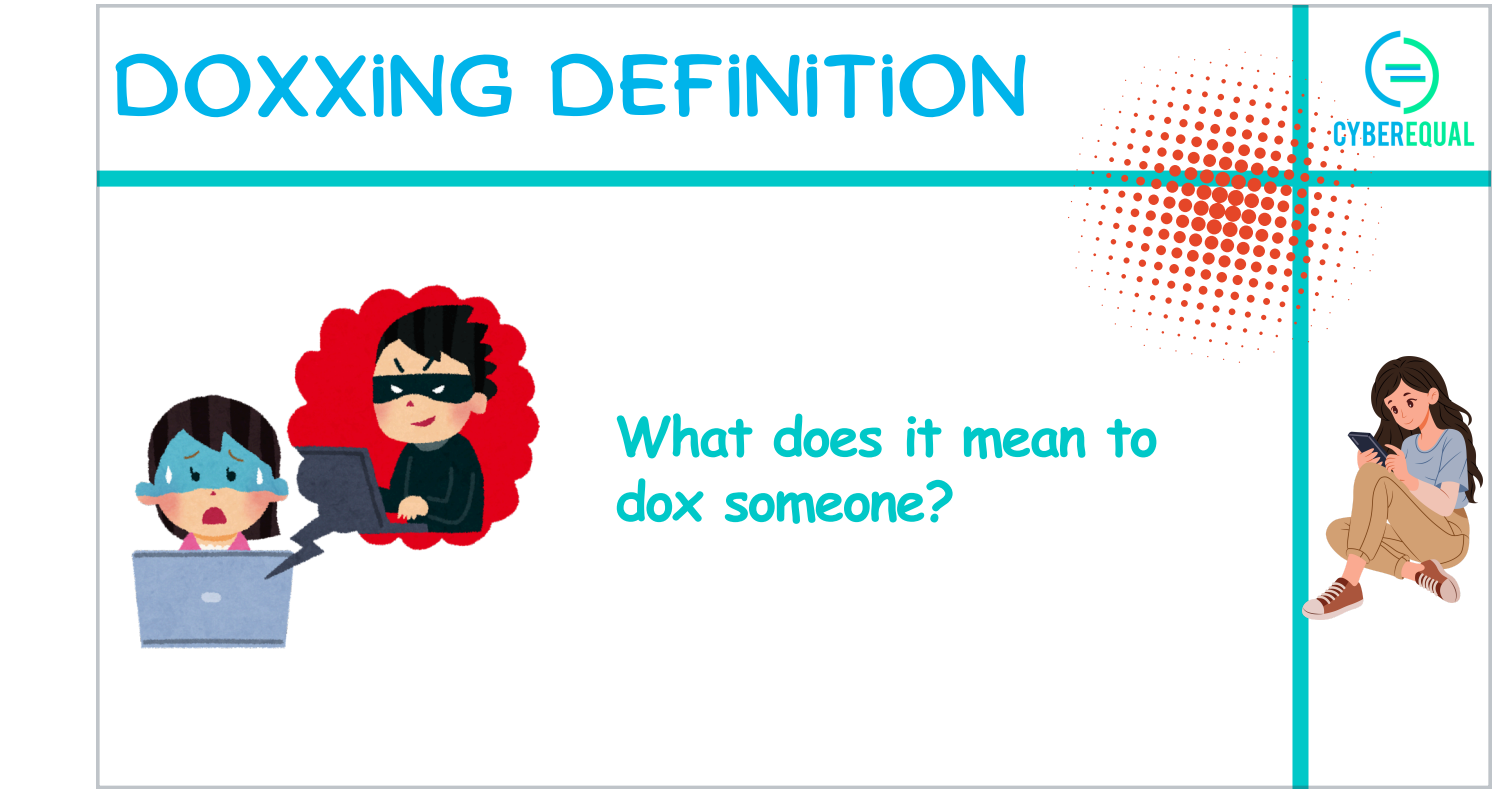
38-year-old Female Arrested

- The victim and the arrested person had an intimate relationship
- They broke up and a few days later, a signboard containing the personal data of the victim was displayed in a street near the victim's workplace, alongside some negative comments against him, including a claim to demand repayment of debt from the victim.
- Shortly afterwards, flyers with similar contents were posted outside the victim's residential building and his flat.
- A message with similar contents was also posted in an open discussion group on a social media platform.

https://www.pcpd.org.hk/english/news_events/media_statements/press_20240705.html

Present the example to the participants and ask if they can identify to which CVAWG threat, the example is referring to.

* You can read the full incident by clicking on the link available on the slide.



Reveal that the threat the example is referring to is Doxxing and ask them if they know what it means to dox someone and if they have ever heard this term before.

*This question helps to more effectively understand the concept of doxxing. Therefore, it is useful facilitators to give participants time to think and provide answers and examples.

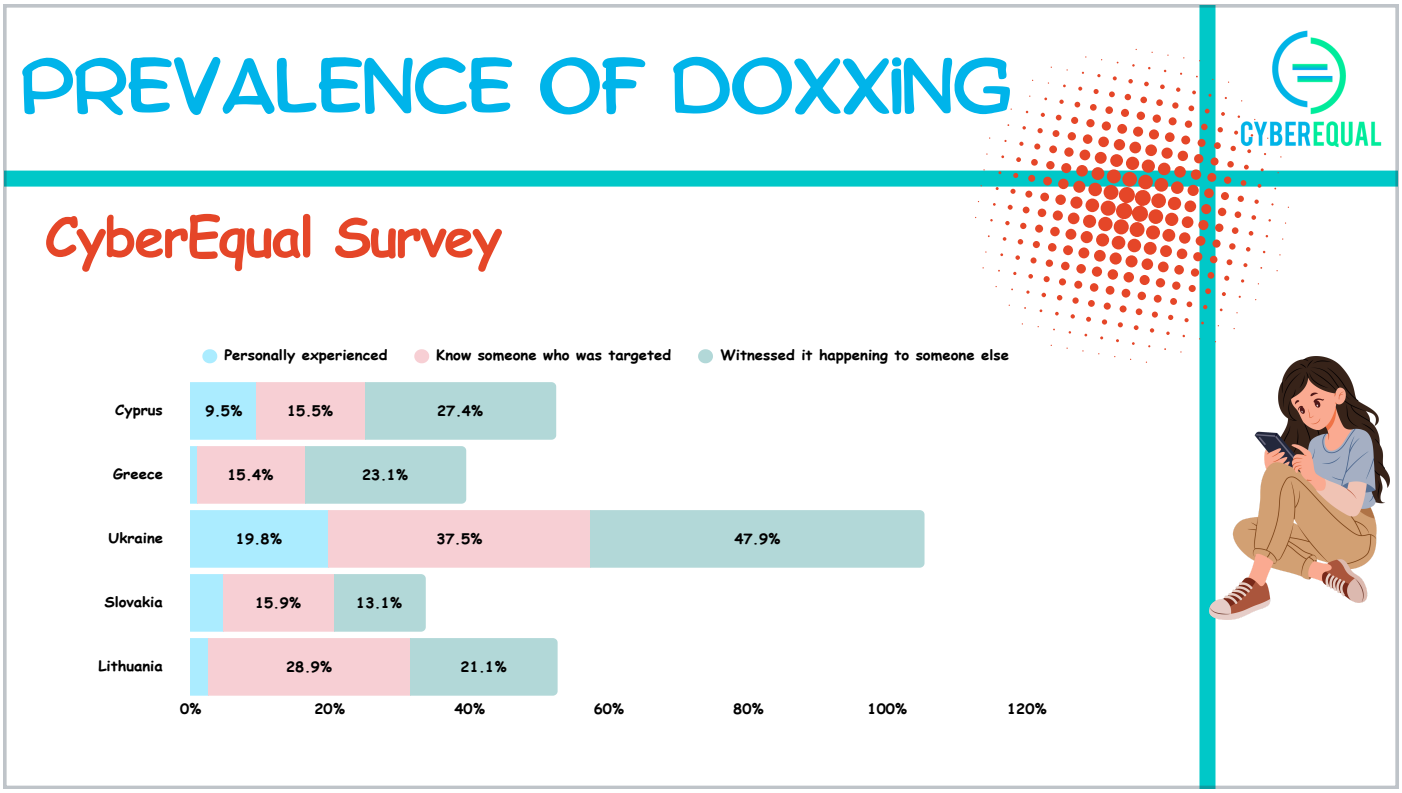
DOXXING DEFINITION

CYBEREQUAL

Doxxing is the intentional publication of a woman's or girl's private personal information online without consent, often accompanied by threats or harassment, and used as a tool of intimidation and violence in digital spaces.

At this point, it can be asked whether participants are aware of any known doxxing cases.

Additional information about Doxxing that facilitators could share:
The concept of doxxing as we currently know it first emerged in the online world in the 1990s, when anonymity was considered sacred. Feuds between rival hackers would sometimes lead to one deciding to "drop docs" on another, who had previously only been known as a username or alias. "Docs" became "dox" and eventually became a verb by itself.

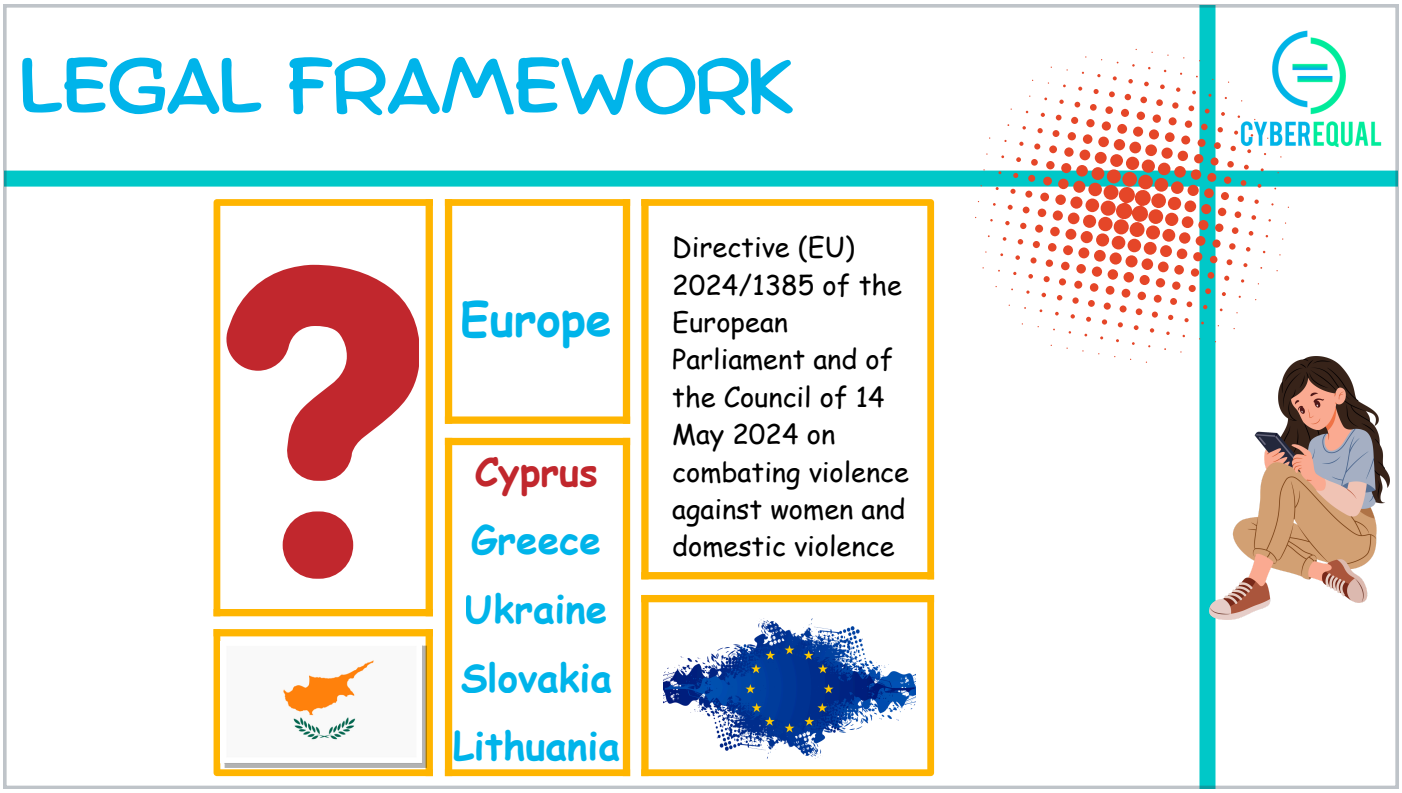


According to recent studies, nearly 1 in 3 women worldwide have experienced some form of gender-based violence.
And with the rise of digital technology, many face violence online too, from harmful messages to threats.

The CVAWG survey was implemented in the context of the 'CyberEqual' project, a project co-funded by the Erasmus+ Programme of the European Union, aiming to map the prevalence of Cyber Violence Against Women and Girls in Cyprus, Greece, Ukraine, Slovakia and Lithuania. 467 women,aged 15 to 35 years old, participated in the study 76% of them reporting having experienced, witnessed, or knowing someone who experienced CVAWG.

In terms of Doxxing the prevalence per country is shown in the current figure.

These numbers show that CVAWG isn't just happening in one place; it's a global problem affecting millions across different countries and communities.

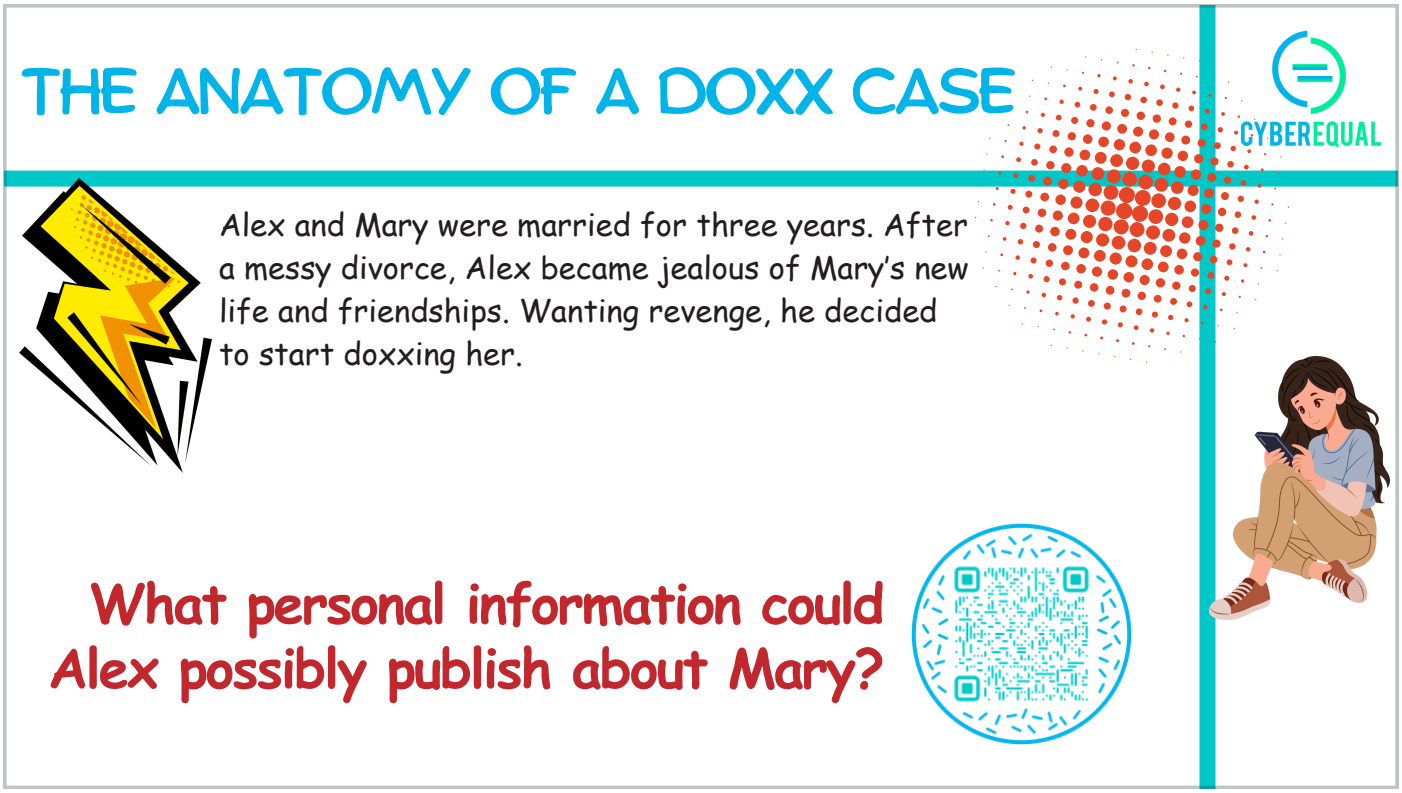


Partners should include their country's legislation on the threat addressed (replace the question mark, the flag and keep their country's name on the box). Another slide maybe added if necessary.

Make clear that the European legal framework is not sufficient for Doxxing.

Could be mentioned:
Unfortunately, a reference to the phenomenon of doxxing in European legislation is only found in DIRECTIVE (EU) 2024/1385 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 May 2024 on combating violence against women and domestic violence and is as follows:
The minimum rules on the offence of cyberbullying should also include rules for situations in which the personal data of the victim are made publicly available through ICT, without their consent, with the aim of inciting other persons to cause physical or serious psychological harm to the victim ("doxing").

However, it is very useful to refer to the national legal framework of each partner country on the subject.

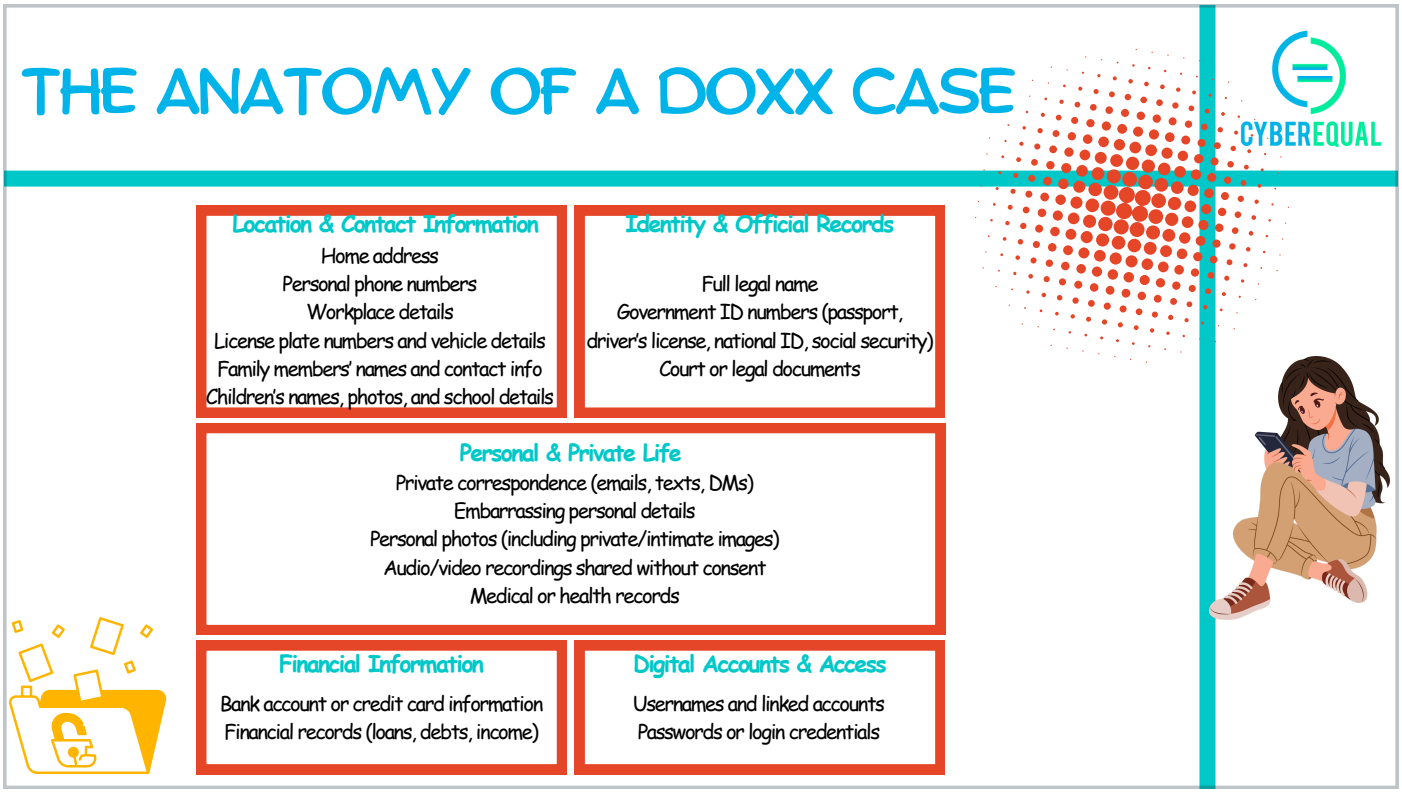


Present the short scenario about Mary and Alex to the participants.

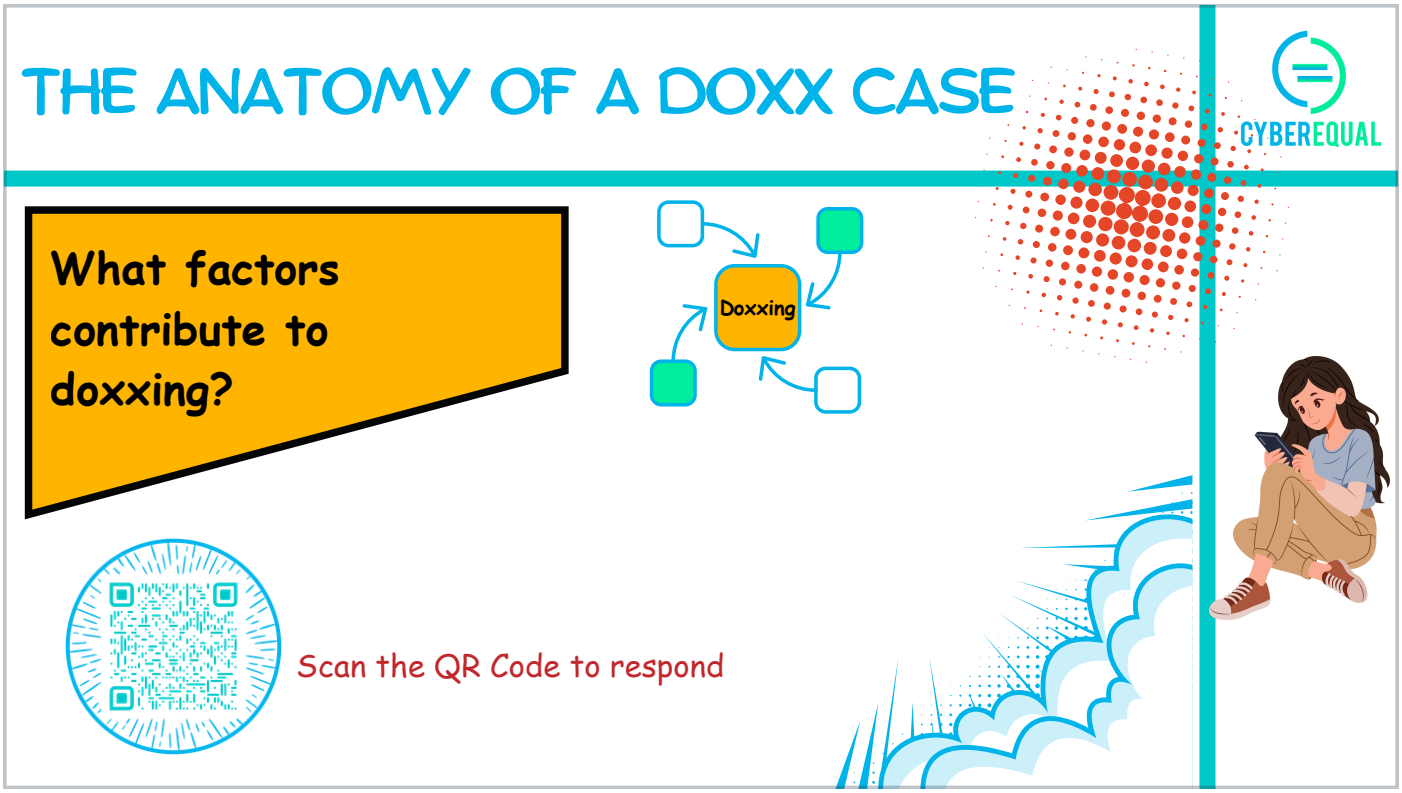
Ask participants to scan the QR code and respond to the question "What personal information could Alex possibly publish about Mary?".

Give participants about 5–7 minutes to write their responses. Once time is up, we read the answers provided by the participants and then move to the next slide to reveal the anatomy of a doxx case.

*In case there is no possibility to create a Slido, use pieces of paper instead, and ask a few participants to read out loud their responses.



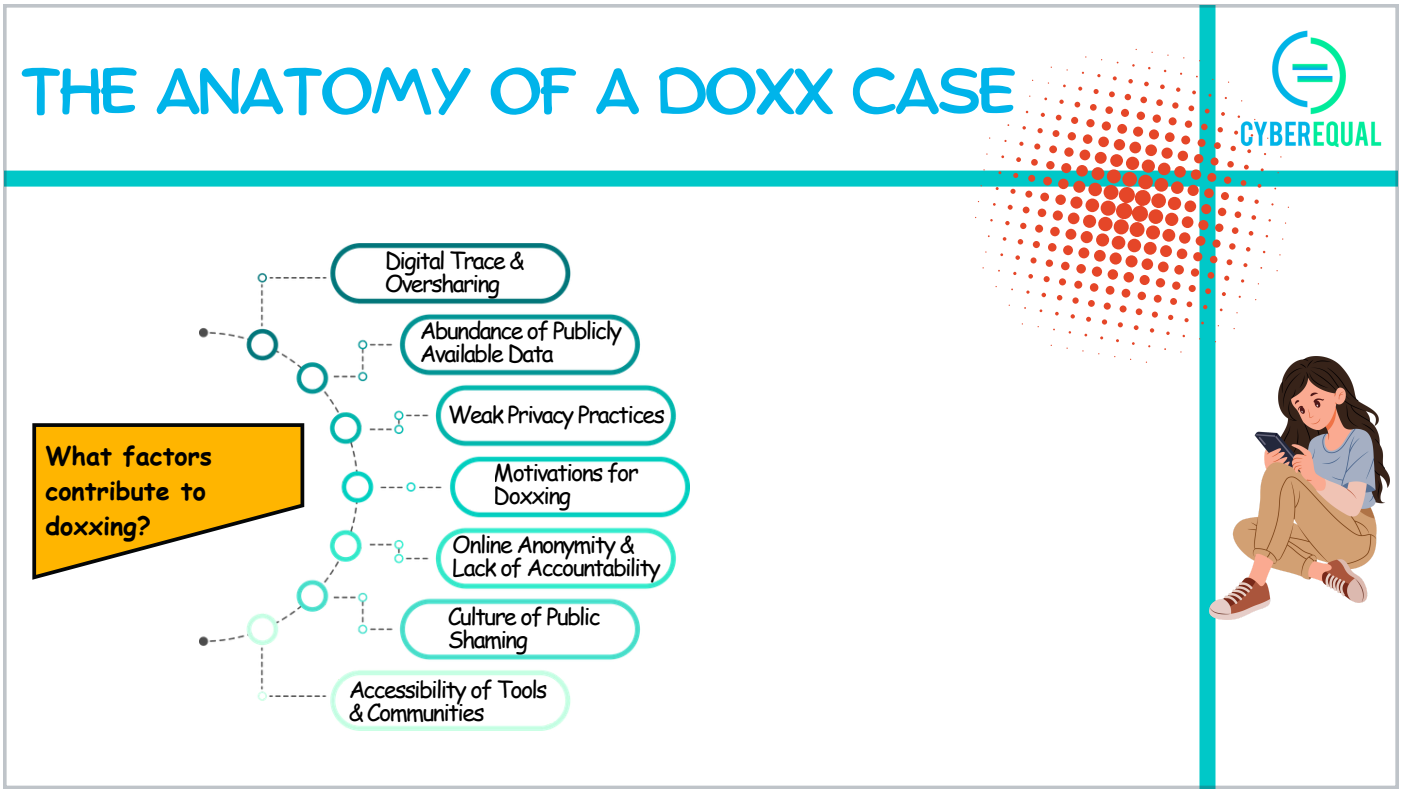
Present the personal data that could possibly be used to doxx someone emphasising that participants should be aware of them, in order to be able to recognise a doxxing incident.



Ask each participant to think and answer through Slido factors that could contribute to doxxing.

* Alternatively, ask them to write the factors on a sticky note, noting one factor per sticky note.

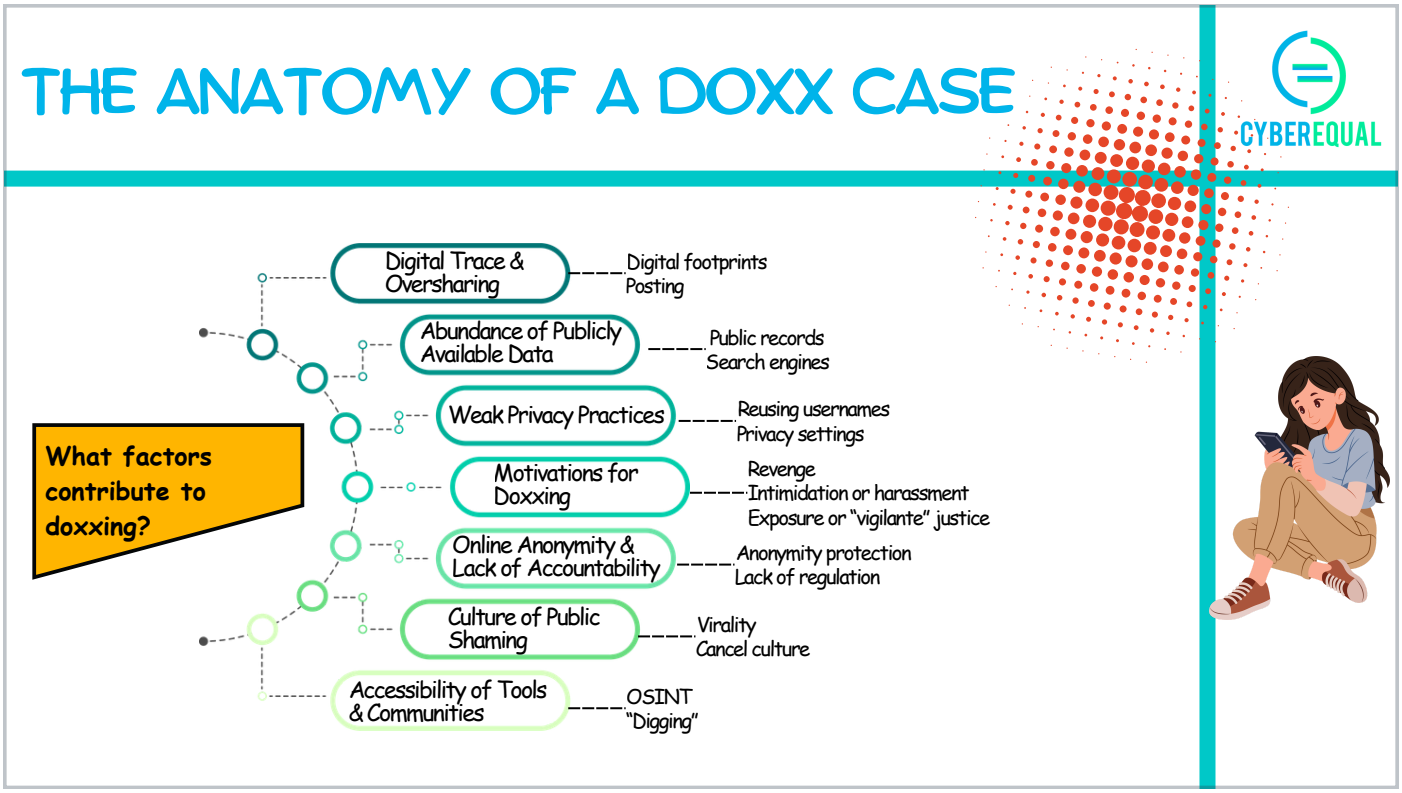
Encourage them to think broadly:
* Personal behaviors (e.g., oversharing)
* Technology (e.g., reverse image search)
* Social or cultural influences (e.g., cancel culture)
* Motivations (e.g., revenge)



Present the generic factors that contribute to doxxing.

Split participants into groups, and ask them to cluster the components of each of the general factors using Mural or by writing them down on a piece of paper.

After 6-7 minutes ask to appoint a representative to present their outcomes.



Go through the details on the factors that contribute to doxxing:

1. Digital Trace & Oversharing

* People leave digital footprints on social media, forums, and websites without realizing how much they reveal.
* Posting photos, geotags, and personal milestones makes it easier for others to piece together private details.

2. Abundance of Publicly Available Data

*Public records, business directories, and leaked databases are readily accessible online.
*Search engines, reverse image tools, and people-finder sites make it simple to connect scattered i nformation.

3. Weak Privacy Practices

*Reusing usernames, having open social media profiles, or using the same photo across platforms creates cross-linking opportunities.
*Lack of awareness about privacy settings leaves accounts exposed.

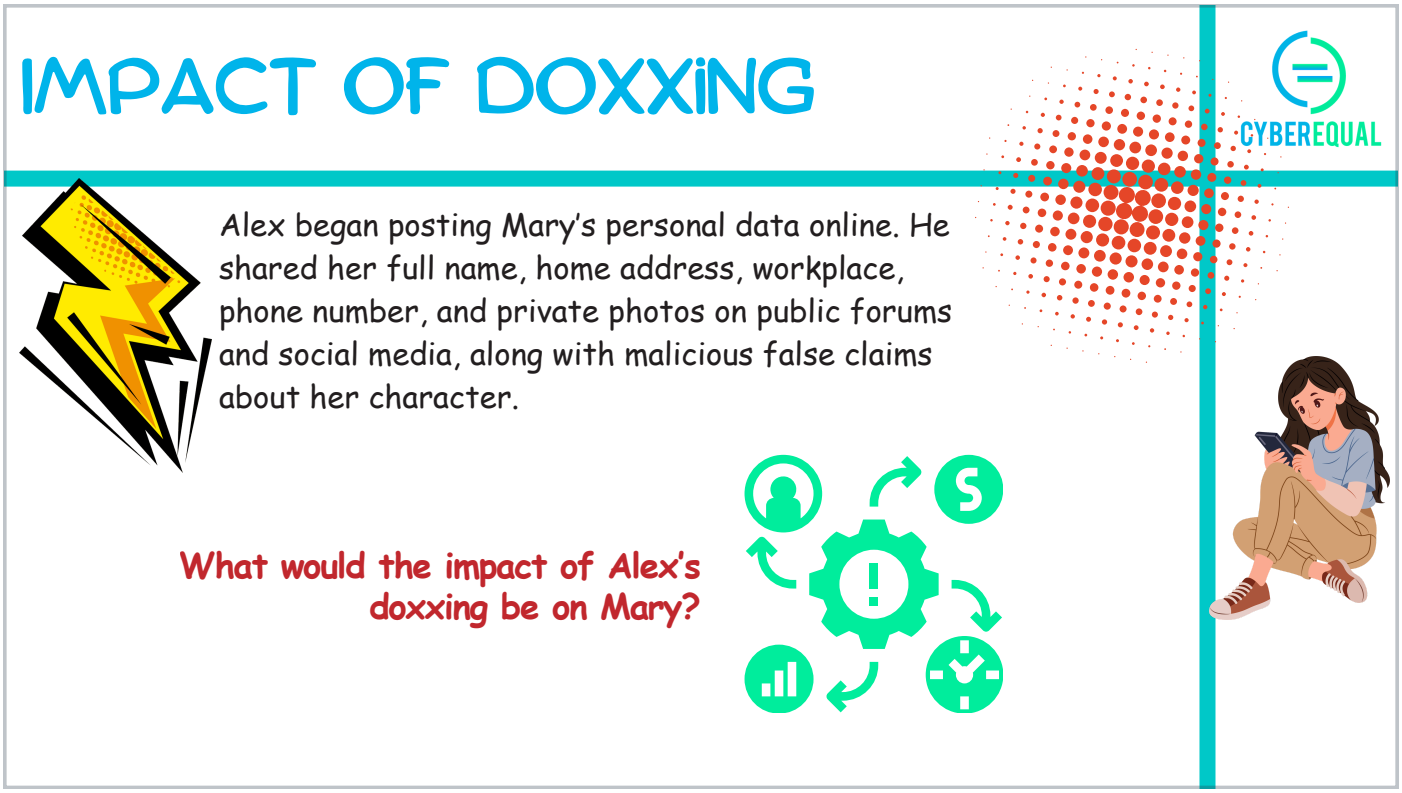
4. Motivations for Doxxing

*Revenge (after breakups, arguments, or conflicts)
*Ideological differences (politics, activism, social causes)
*Intimidation or harassment (cyberbullying, silencing critics)
*Exposure or "vigilante" justice (trying to hold someone accountable — justified or not)
*Entertainment or clout (shock value, online notoriety)

5. Online Anonymity & Lack of Accountability
*Perpetrators often feel protected by anonymity, believing they won't face real-world consequence s.
*Many platforms lack strong enforcement against doxxing, making it easier to get away with.

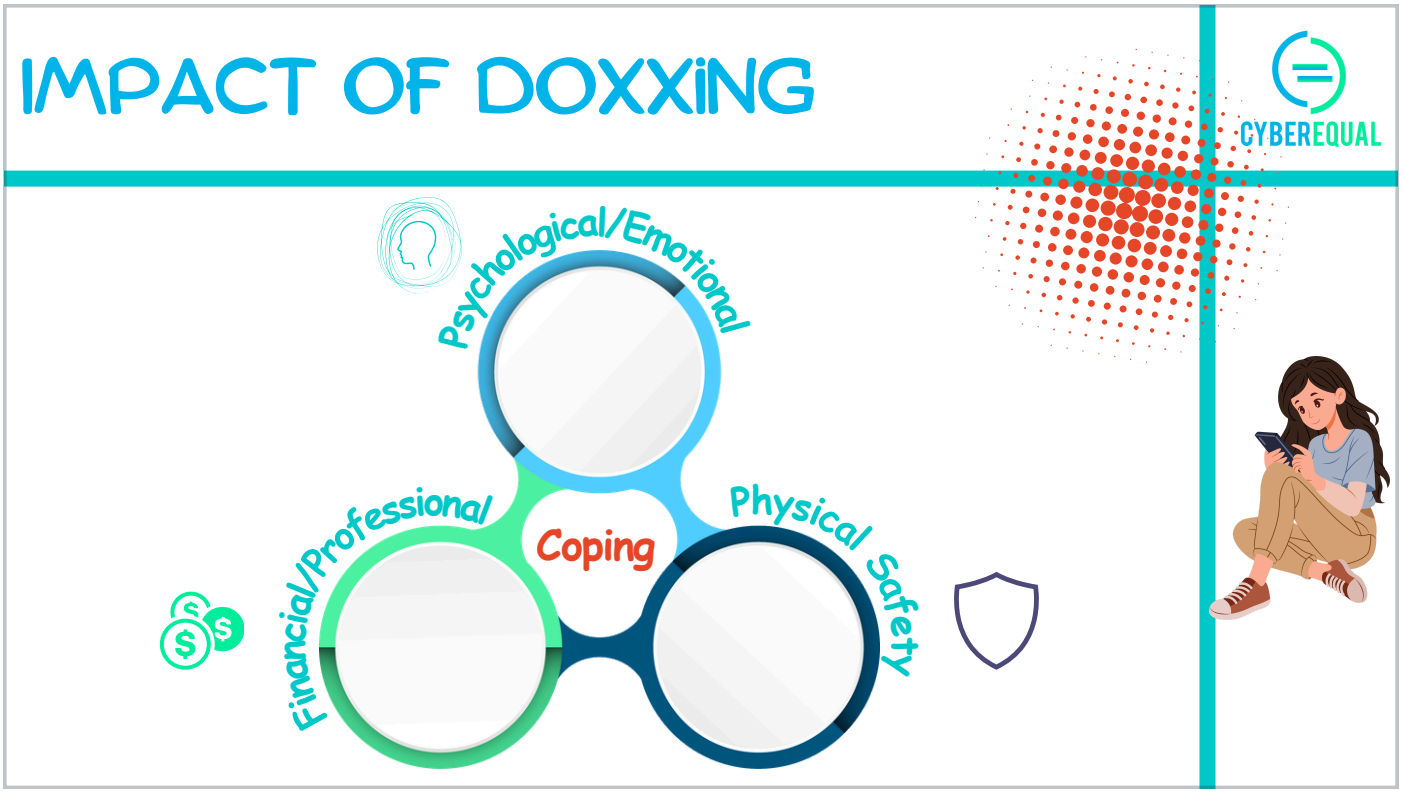
6. Culture of Public Shaming
*Social media thrives on outrage and virality.
*Doxxing is sometimes used as part of a "cancel culture" mindset, where exposing someone is seen as a form of justice.

7. Accessibility of Tools & Communities
*OSINT (Open-Source Intelligence) tools are free and easy to use.
*Online communities dedicated to "digging" can work together to gather and verify personal inform ation.

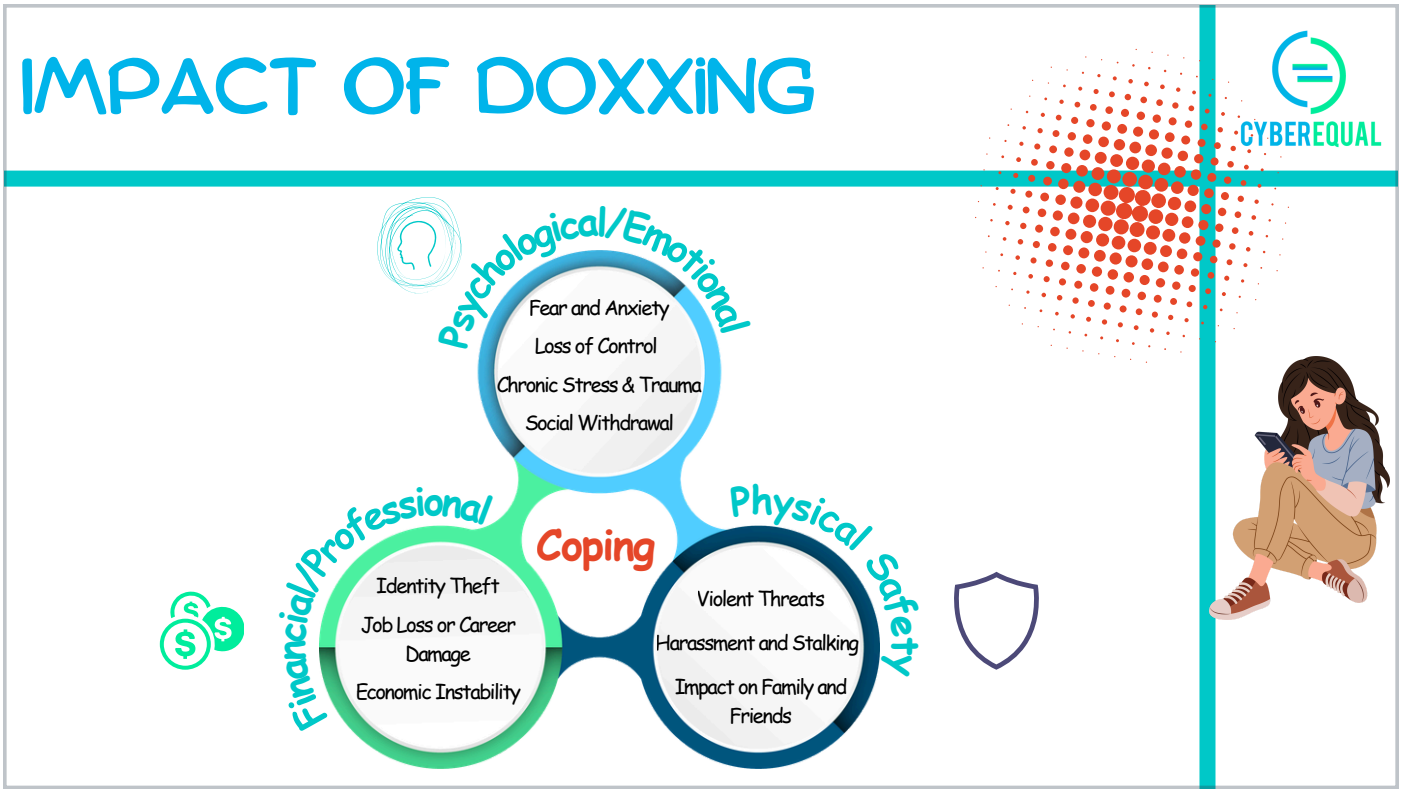


Let's delve into the impact of doxxing, focusing on Mary's case.

Imagine the overwhelming sense of vulnerability and fear when your personal information is exposed online without consent. Alex's actions, posting her full name, home address, workplace, and phone number, create a profound breach of privacy.



Guide their thinking using the three presented impact categories.

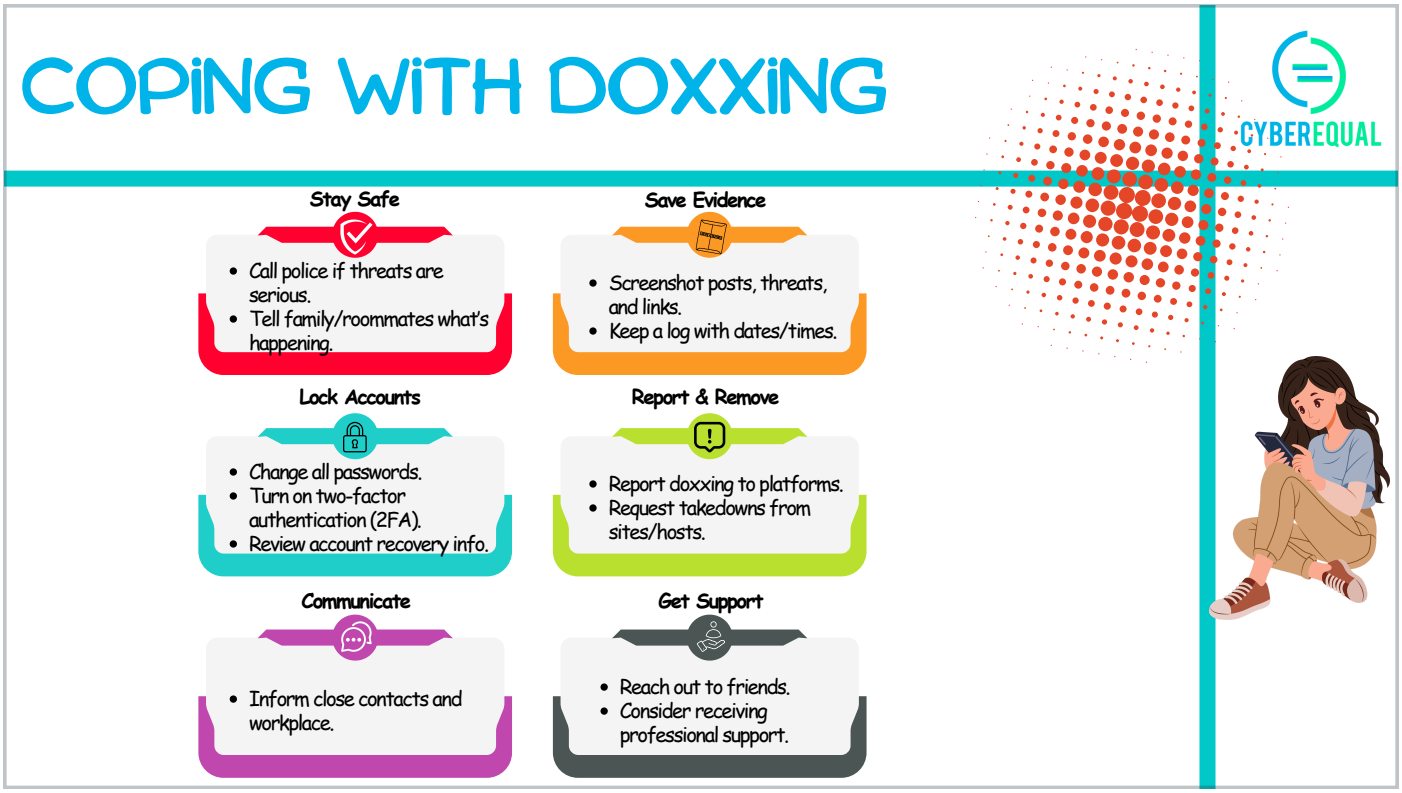


Firstly, consider the emotional toll. Being publicly shamed and having false claims spread about her character can lead to severe psychological distress. This may result in anxiety, depression, and a significant loss of trust in online interactions.

Now, think about the professional impact. Such exposure could jeopardize Mary's job and professional reputation, potentially leading to job loss or difficulty in future employment. The spread of private information can also facilitate identity theft, adding financial strain.

Lastly, consider the implications for physical safety. With personal details widely accessible, Mary faces increased risks of harassment, stalking, or even violent threats.

Doxxing isn't just a digital attack; its repercussions ripple into every facet of the victim's life.



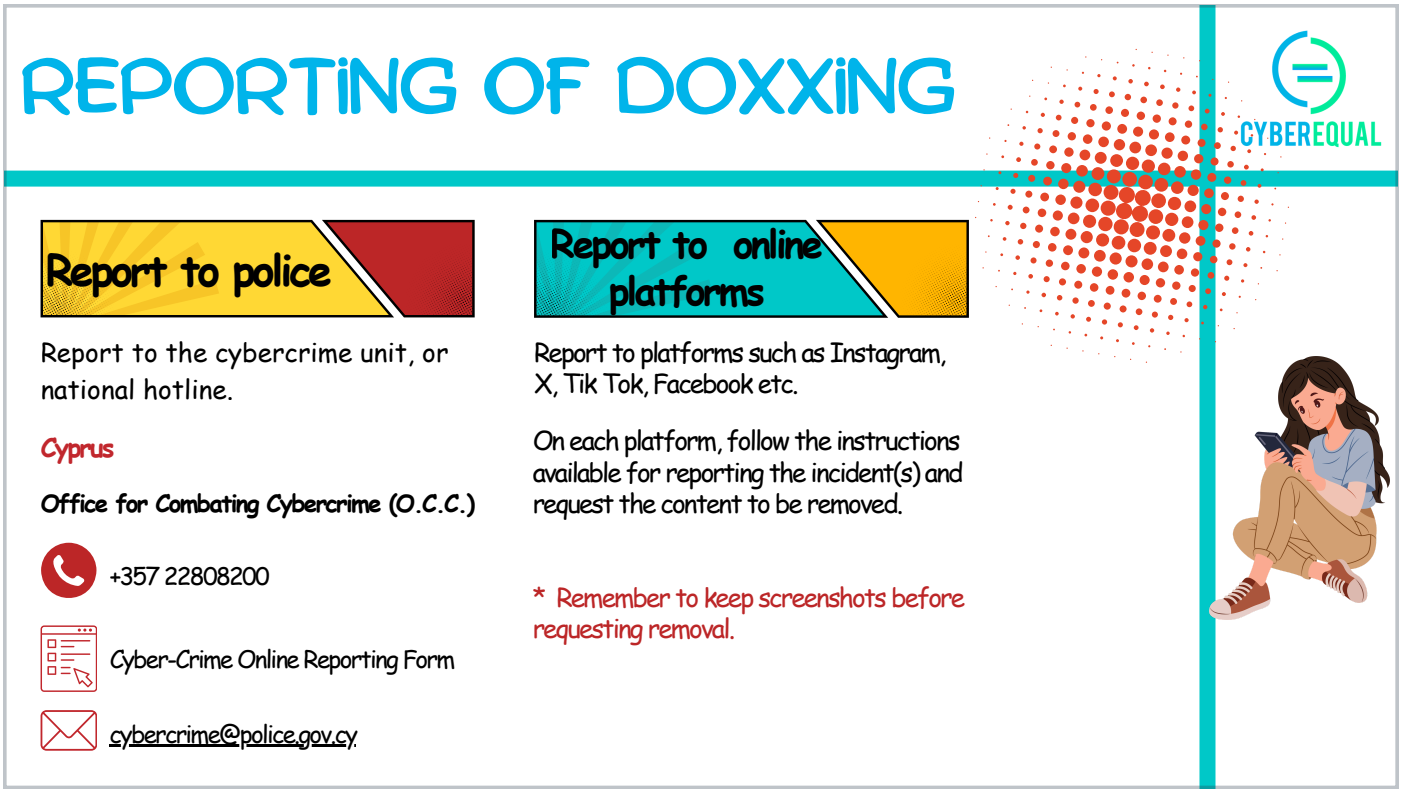
Let's focus on practical steps for coping with doxxing. It's crucial to reach out to your support network, so consider talking to friends, family, or roommates about what's happening.

If threats become serious, contacting the police is essential. Document everything; screenshot any posts, threats, and links, and maintain a detailed log of dates and times. This evidence can be crucial later on.

Security is paramount. Change all your passwords and enable two-factor authentication on your accounts. Ensure your account recovery information is up-to-date as well.

Reporting and removing intrusive content is another key step. Reach out to online platforms and request takedowns of harmful material. Keep your close contacts and workplace informed to ensure your safety and support.

Finally, don't hesitate to seek professional support if needed. Remember, you're not alone in this, and there are resources available to help you navigate these challenges.



** Each partner should replace the country, police unit and contact details.**

In the unfortunate event of a doxxing incident, it is important to know where and how to report. Although doxxing is often not a separate crime, it is treated as a personal data offence.

First and foremost, it's crucial to report to the right authorities, starting with the cybercrime unit or national hotline. This ensures your case is handled by professionals who can offer the best guidance and support.

When you're reporting, remember to include your local police. They're an essential part of the process, especially if you feel your safety is at risk.

Don't forget about reporting to online platforms. Each one, like Instagram, X, TikTok, and Facebook, has specific instructions for handling these reports. It is vital to follow their steps precisely to have the content removed.

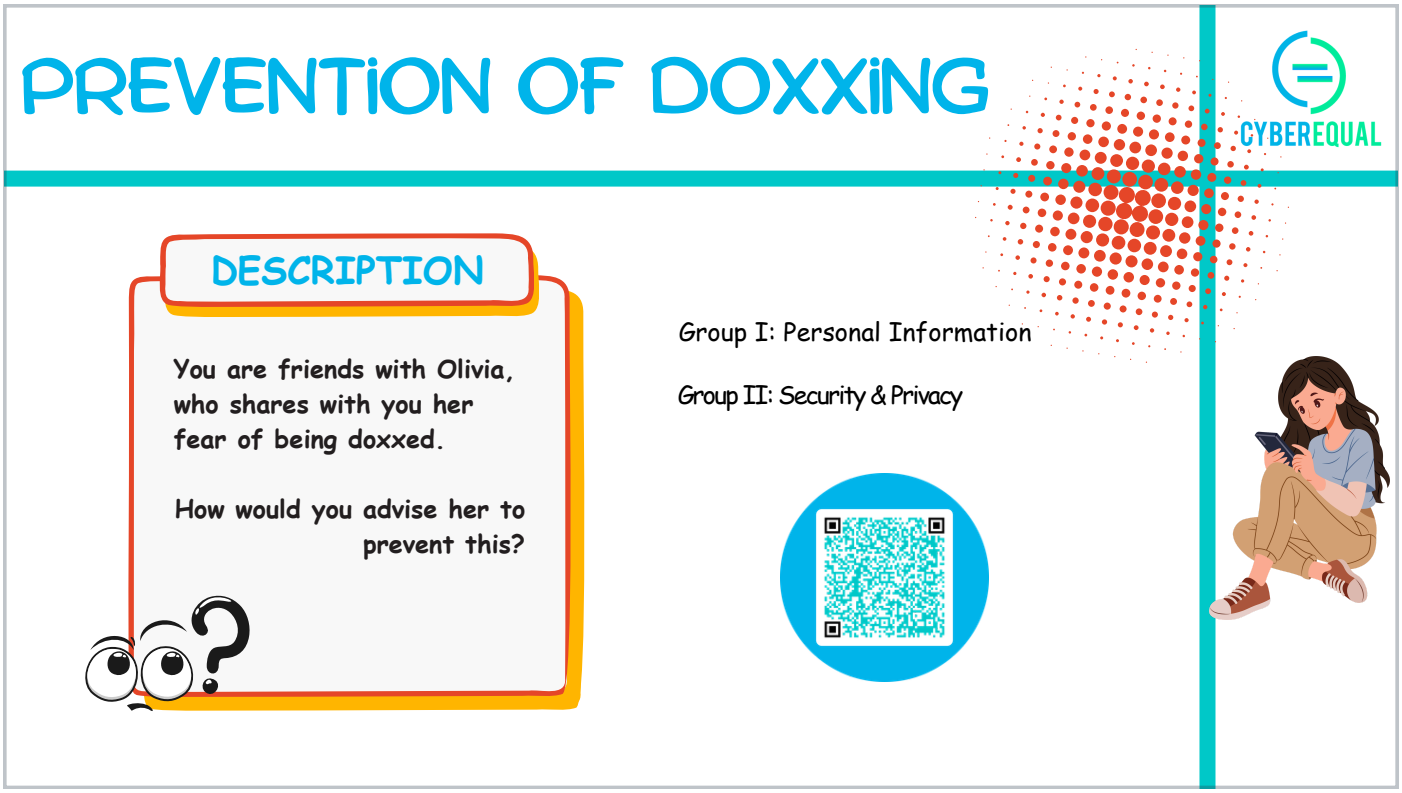
Before you request content removal, always keep screenshots. This serves as crucial evidence if you need to escalate the issue further.

By taking these steps, you're not just protecting yourself but also contributing to a safer online community. Do you have any questions before we move on?

PREVENTION OF DOXXING

CYBEREQUAL

THE COUNSELING CENTER



Inform the participants that this is a hypothetical scenario for which they should answer by creating a brochure with prevention measures Olivia should follow in order to prevent being doxxed.

Split participants into two groups and ask them to create their part of the brochure (allocate one section per group) using the Canva link provided or to design it on a piece of paper.

Give participants 10 minutes to complete it, then discuss what they have created.

PREVENTION OF DOXXING

CYBEREQUAL

Personal Information

- Avoid posting under your full legal name unless necessary.
- Keep professional, personal, and anonymous accounts distinct.
- Restrict profile visibility, friend lists, and past posts to trusted contacts on social media.
- Turn off geotagging in apps and remove location metadata from posts/photos.
- Use separate emails for banking, work, and public sign-ups.

Security / Privacy

- Use a password manager to avoid reuse across accounts.
- Use providers with strong anti-phishing protections; set up recovery options carefully.
- Do not engage in doxxing as responding to harassers often escalates the situation.




CYBEREQUAL

THANK YOU

CVAWG IS REAL VIOLENCE!

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.