DOXING & SOCIAL MEDIA PRIVACY FACT SHEET

COMMUNITY SECURITY GROUP
NEW SOUTH WALES

If you feel threatened or are at risk of immediate harm, call 000.

What is Doxing?[1]

Doxing is the intentional online exposure of an individual's identity, private information or personal details without their consent.

Sharing the information publicly undermines the target's privacy, security, safety and/or reputation. Often those responsible for doxing urge others to use the information to harass the person targeted.

Revealing private information about a person without their consent is not new. However, the increased use of internet connected technologies has made it far easier to collect, store, track and then share the information very publicly. The growth of online platforms has also expanded the network of people able to harass, humiliate or attack someone once their identifying details have been revealed.

Doxing is an abbreviation for 'dropping documents'. The information that is doxed may be sourced through publicly available information, research of public records or through unauthorised access to private databases and computer systems (hacking).

Unlike defamation, doxing does not have to reveal something untrue or damaging about an individual — the information is usually accurate, whether or not it has been sourced lawfully.

'Doxing' can refer to a number of different practices.

Deanonymizing doxing:
Revealing the identity of someone who was previously anonymous (for example, someone who uses a pseudonym).

Targeting doxing:
Revealing specific information about someone that allows them to be contacted or located, or their online security to be breached (for example, their phone number or home address, or their account username and password).

Delegitimizing doxing:
Revealing sensitive or intimate information about someone that can damage their credibility or reputation (for example, their private medical, legal, or financial records, or personal messages and photos usually kept out of public view).

Why do people dox?
Research points to a variety of motivations for doxing. In some cases, doxing is motivated by wanting to expose wrongdoing and hold the wrongdoer to account. It can also be used to exert control over someone following a relationship breakdown.

The threat of doxing can also be used to intimidate or threaten someone. In some cases, it is used to extort money, but often no demands are made to stop the information being released and the target is not even aware they are about to be doxed.

Anyone can be doxed and, regardless of the motive, the exposure of personal information violates the target's privacy and can compromise their safety. Reports of doxing made to eSafety indicate that it can lead to serious emotional, psychological and physical harms.

[1] https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing

DOXING & SOCIAL MEDIA PRIVACY FACT SHEET

COMMUNITY SECURITY GROUP
NEW SOUTH WALES

What harm can doxing cause?

Doxing can leave the target vulnerable to, and fearful of:

- public embarrassment, humiliation or shaming
- discrimination, if personal characteristics are disclosed
- cyberstalking and physical stalking
- identity theft and financial fraud
- damage to their personal and professional reputation, leading to social and financial disadvantage
- increased anxiety
- reduced confidence and self-esteem.

The harms can be immediate, but they can also be ongoing if the information continues to be shared or stored by others.

On a broader level, using doxing as a form of digital vigilantism can have a negative impact on society through increasing lawlessness, conflict and reducing trust in public figures.

How to protect yourself against doxing:

- Check privacy settings on social media accounts, ensuring that you know who can see the content you share and who has access to your personal information.
- Use a range of strong passwords for your accounts, and ensure that any security questions are sufficiently difficult to guess.
- Try to use 'passphrases' instead of passwords and change them regularly.
- Avoid using the same password across multiple platforms.
- Try to set unique usernames for each online account you use.
- Use secure authentication on all accounts, including two-factor authentication where available.
- Limit the amount of personal information that you share online, such as your address, place of work or study, or personal phone numbers.
- Make a habit of searching for yourself online in incognito mode, to see how much of your information is accessible to others.

What to do if you are doxed:

- Collect and preserve evidence of the doxing. Take screenshots which include the individual/s name/s who are sharing information about you. This will help demonstrate what occurred and may be required as official evidence should it need to be escalated.
- Report to the social media platform where the doxed material is posted. Use this guide to find the relevant resources to assist: https://www.esafety.gov.au/key-issues/esafety-guide
- Block unwanted contact.
- Seek further support from:
  eSafety: https://www.esafety.gov.au/report (In Australia, the eSafety Commissioner is the regulatory body responsible for online safety.)
  Crime Stoppers: https://www1.police.nsw.gov.au/cs.aspx
  CSG NSW: https://www.csgnsw.org.au/report

Remember, if you feel threatened or are at risk of immediate harm, call 000.

Is Doxing illegal?

In February 2024, Australian Prime Minister, Anthony Albanese, confirmed that his government will support a proposal to make doxing illegal.

Be aware of what you share:

Consider how much information you share online, where you share it, and who you share it with. Be mindful of who you are connecting with and regularly review your privacy settings.

You should also be aware that, depending on your privacy settings, users may be able to see when you view their posts on some social media platforms.

WhatsApp group privacy settings:

WhatsApp groups have become a convenient way for like-minded individuals to come together and share news, opinions, suggestions and information.

It is essential that we all consider these groups as 'open' – with all members having the ability to screenshot and forward messages, profile photos and phone numbers.

By default, your group privacy settings are set to **Everyone**. This way, you can easily connect with friends and family, even if they're not in your contacts list. For additional privacy, you can control who can add you to a group by adjusting your WhatsApp Settings.

- Changes to group privacy settings can't be made on WhatsApp Web or Desktop. When you change the settings on your phone, they will be synced with WhatsApp Web and Desktop.
- This setting doesn't apply to community Announcements. When you're in a community, you'll always be added to community Announcements.

Change group privacy settings:

1. Tap **Settings**.
2. Tap **Privacy** > **Groups**.
3. Select one of the following options:
    - **Everyone**: Everyone, including people outside of your phone's address book contacts, can add you to groups without your approval.
    - **My contacts**: Only contacts in your phone's address book can add you to groups without your approval. If a group admin who's not in your phone's address book tries to add you to a group, they'll get a pop-up that says they can't add you and will be prompted to tap **Invite to group** or press **Continue**, followed by the send button, to send a private group invite through an individual chat. You'll have three days to accept the invite before it expires.
    - **My contacts except...**: Only contacts in your phone's address book, except those you exclude, can add you to groups without your approval. After selecting **My contacts except…** you can search for or select contacts to exclude. If a group admin you exclude tries to add you to a group, they'll get a pop-up that says they can't add you and will be prompted to tap **Invite to group** followed by the send button to send a private group invite through an individual chat. You'll have three days to accept the invite before it expires.
4. If prompted, tap **Done**.

DOXING & SOCIAL MEDIA PRIVACY FACT SHEET

COMMUNITY SECURITY GROUP
NEW SOUTH WALES

Information Sources & Further Information

Securing Your Social Media:
https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/user-education/security-tips-social-media-and-messaging-apps

Social Media & Privacy:
https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/social-media

Collecting and Preserving Evidence:
https://www.esafety.gov.au/report/how-to-collect-evidence

Doxing Resources:
https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing

Cyber Security:
https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides

Facebook Privacy Settings:
https://www.facebook.com/help/325807937506242

Instagram Privacy Settings:
https://help.instagram.com/811572406418223

WhatsApp Privacy Settings:
https://faq.whatsapp.com/3307102709559968/?cms_platform=web

LinkedIn Privacy Settings:
https://www.linkedin.com/help/linkedin/answer/a1337839