



Doxing and Data Privacy Implications



What is Doxing?

It is an act of researching and publicly revealing private or personal information about an individual without their consent, often with malicious intent.



Common Targets

- Everyday internet users
- Content creators & influencers
- Journalists & activists
- Gamers & online community members









Why It's Dangerous

- Identity theft
- Harassment & stalking
- Damage to reputation & career
- Physical safety risks

How to Protect Yourself



-  Use strong, unique passwords & 2FA
-  Limit personal info shared online
-  Check privacy settings regularly
-  Avoid posting location in real time
-  Use a VPN for extra privacy
-  Be cautious of suspicious links & requests



How Doxing Happens

- Social Media: Oversharing personal details
- Data Breaches: Leaked databases & accounts
- Phishing: Trick emails & messages
- OSINT: Open-source intelligence (search engines, public records)



Legal & Ethical Side

- Doxing can violate privacy laws and lead to criminal charges.
- It's considered a form of cyber harassment.



Resources

- Privacy International – Doxing Explained
<http://bit.ly/46hdsrD>
- National Cybersecurity Alliance – Protecting Your Digital Identity
<https://www.staysafeonline.org/>
- Federal Trade Commission – Avoiding Phishing
<http://bit.ly/45POyiN>