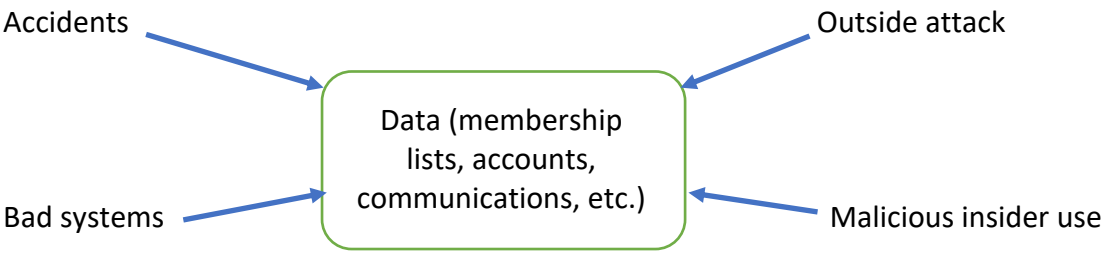
Making your data secure

Ideas for campaigners

What it's about

You're involved with a group campaigning on human rights, environment, social welfare or some other cause. You're aware of the Australian government's capacity for surveillance and disruption of your communications and data, including the Australian Federal Police's power to access, delete, modify or add to your data.

What are your options to make your group's data more secure?



SAMPLE SCENARIOS

Accident Your membership list, an Excel spreadsheet, is kept on the same computer used to send messages to all supporters. When adding an attachment to a message, the membership list — including names, phone numbers, payments and personal details — is accidentally sent to all supporters. This embarrasses some members and puts a few at risk.

Bad system All your confidential files are kept in an encrypted folder under the control of a trusted, long-time office-bearer. She has an accident. You are not able to retrieve any of the information.

Outside attack One of your members, Jones, is paid by the police to collect information about your members' activities. Jones seems highly loyal and hard-working and is given access to financial and personal files. The police, with this information, covertly harass some of your members.

Malicious insider use Your organisation collects lots of personal information. Two of your members, J and K, who have been in a close relationship for years, break up and have horrific battles. J uses access to the organisation's database to make contact with members from around the world and send damaging messages about K.

Why keep data?

- Need for activities
- Archive
- Legal or organisational requirements
- Habit
- Hoarding

What sort of data might be targeted for surveillance or disruption?

Commercial, national security, medical, private, whistleblowing

Option	Strengths	Weaknesses or costs
Extra authentication procedures	Protects from brute force attacks	Inconvenience
Back-ups on the cloud	Protects from loss	Cloud vulnerabilities
Your own back-ups (e.g., external hard drive)	Protects from loss and from cloud surveillance	Maintaining back-ups; targeted attacks
Back-ups with trusted others	Protects from loss and from cloud surveillance	Reliance on others
Encryption	Protects from easy outsider access	Inconvenience; social engineering; keyloggers
Limit access to a few members	Reduces risk of accidents and malicious insider use	Members with access may gain undue influence; divisiveness
Destruction of data	Protects from surveillance	Loss of data

Considerations

Things to take into account when developing or assessing your group's data security practices:

- If your data is compromised, is anyone in jeopardy?
- How much time and effort does it take to back up your data?
- Does your group have adversaries who might seek to access or alter your data?
- What vulnerabilities does your group have? Think of reputations, finances, blackmail, internal rifts, skill shortages.

Info sheet #3
Resistance Resources
https://bit.ly/3ouoYtw
This version 7 February 2022

Comments are welcome to improve and update this info sheet.
Contact Brian Martin, bmartin@uow.edu.au