CYBER SECURITY AWARENESS MONTH · OCTOBER 2026

Protect your research in the AI era

What you share with an AI tool may leave your control. Depending on the service and its settings, unpublished ideas could be retained, used to train future models and later resurface in answers to other people, detached from your name.

Before you share, ask: is it worth the risk?



1. Your unpublished idea goes into an AI service.
2. If it is retained or used in training...
3. ...it could resurface in someone else's answer, with no author named.

Before you share with AI

Decide whether to share, and what.

1 Protect your unpublished contribution

Is this your core unpublished idea, and could losing control of it affect your priority or novelty? For potentially patentable work, speak to your IP office first.

2 Spot sensitive information

Does this contain confidential, personal or culturally sensitive data?

3 Check policy and permission

Do my institution's policy, ethics approval, agreements and reviewer confidentiality obligations allow this?

4 Share the minimum

Can I describe the problem, use a generalised example, or leave out the core idea and still get the help I need?

Safer ways to use AI

If you do share, reduce the exposure.

5 Check training and privacy controls

Find out whether your inputs may be used for training, and opt out where the service allows.

6 Check retention, not just the label

Find out how long inputs and outputs are stored. An "enterprise" or "API" label is a reason to check the protections, not a protection in itself.

7 Run it locally, properly configured

Use a fully local set-up with cloud features and external connections switched off. Installing a desktop application alone does not guarantee this.

8 Fence in AI agents

Limit access to an enforced project folder, not your whole drive, email or accounts. Documents and websites can carry hidden instructions that try to redirect an agent.

AI SECURITY HABITS

Assume the entire interaction could be visible to anyone.

- **Sanitise inputs** Strip personal identifiers, credentials and confidential details before you share.
- **Limit permissions** Give AI tools and agents only the access the task needs.
- **Fact-check outputs** Never assume AI-generated summaries, citations or analyses are accurate. Check the original sources.
- **Avoid research misconduct** Fabrication, falsification and plagiarism remain misconduct, even when AI produced the content.

Unsure? Check University policy and ask your supervisor or research team before you share.

CRICOS: 00219C | TEQSA: PRV12073 | RTO: 40939
Icons: Font Awesome

About the authors: Dr Mahmoud Elkhodr and Professor Ergun Gide, CQUniversity Australia.

Further guidance for research candidates and supervisors: SAGE Research Website, **sage-framework.com/sager**