Social Media & Privacy

Understanding Social Media Threats

Who is at risk?

All social media users, including farmers, are potential targets for cybercriminals. Even if you think you are low risk, specialised demographics, such as farmers, can be easily identified and exploited.

Types of threats:

- Misinformation: False information that can damage reputation or mislead others.
- Phishing and social engineering: Attempts to trick you into revealing sensitive information, such as passwords, usernames and farm operations.
- Data mining: Collecting your personal data for malicious purposes

Protecting your social media profile

Profile pages

- **Threats**: Information such as birthdate, location and employment, such as farming, can be used to answer security questions for password recovery, making you vulnerable to hacking.
- **Media risks**: Photos and videos can reveal your farm's location, security flaws and operations. This can potentially lead to financial losses.

Mitigation tips

- Avoid creating social media accounts: Obviously, it is the most secure option, but it is not very practical.
- Limit what you share: Be cautious with what you share and how you engage with other posts online. Even seemingly harmless posts can result in catastrophic losses.
- Lock your profile: Restrict access to your profile to approved people, and only provide limited information.

Privacy and security risks from sharing media

Risks

- Oversharing: Posting too much about your farm operations or new technology can attract cybercriminals
- Image and text misuse: Once online, anything you share can be copied and altered. This can then be used against you to damage your reputation, potentially costing you financially

Mitigation tips

- Careful posting: Avoid sharing your exact location. Operation details, personal or financial information.
- Monitor content: Regularly review what you have shared and remove anything that could be misused.
- Consider the impact: Understand how a simple post could be taken out of context or misused, especially in the age of AI.

Social network privacy settings

Privacy settings control who can see your information and can help protect you from cyber threats

Social Network Privacy Settings

Facebook Privacy Settings

Lock Facebook Profile

Make Instagram Private

Instagram Privacy Settings

LinkedIn Manage Settings

Understand LinkedIn Privacy Settings

LinkedIn Privacy Settings

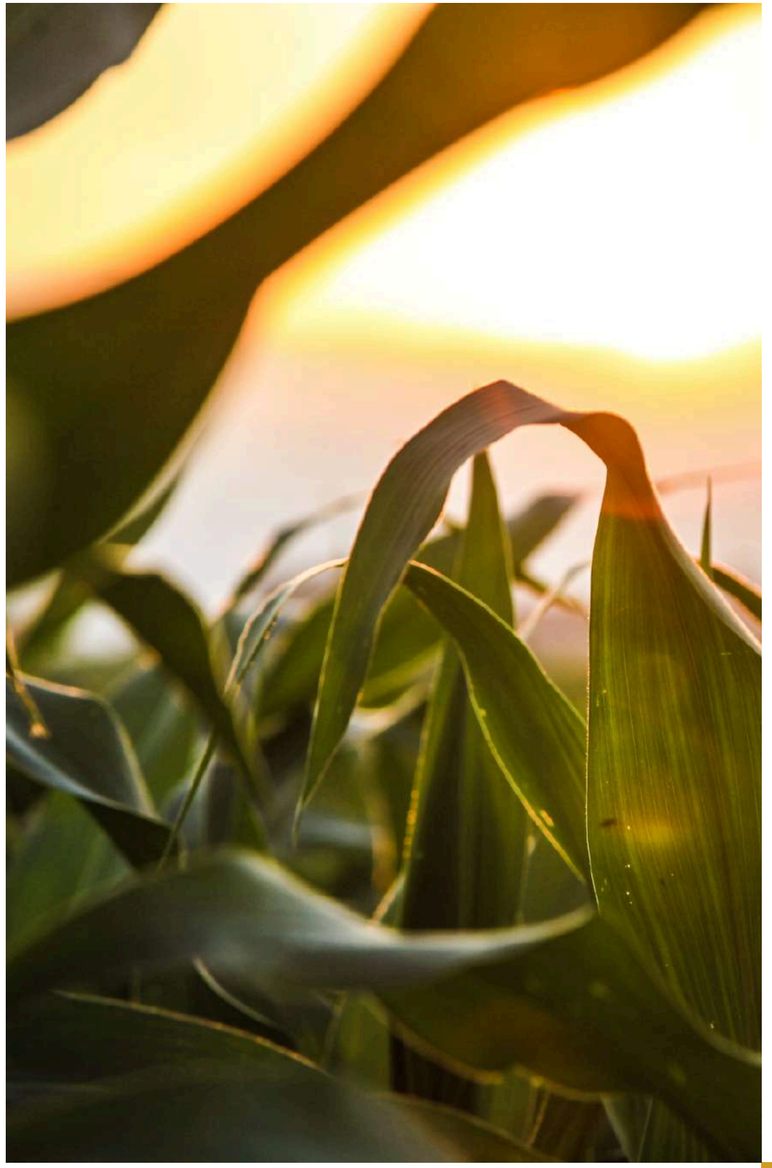
YouTube Privacy Settings

TikTok Privacy Settings

Snapchat Privacy Settings

Tinder Privacy Settings

Reddit Privacy Settings



Avoiding social media scams and phishing

Common tactics

- Fake “fun” posts: Public posts that seem to be harmless but are used to gather sensitive personal information.
- Lost person posts: Often used by scammers to find vulnerable individuals.
- Marketplace scams: Fake sales listings targeting users through urgency, high-pressure tactics and deals too good to be true.

Mitigation Tips

- **Lock your profile**: Protect your personal information and your connections
- **Scrutinise posts**: Verify sources and details before engaging with any listing or post.
- **Inspect sellers**: Before buying on marketplaces or groups, check their profile page for the age of the account, friends and fine details, such as currency symbols and payment methods.
- **Trust your instincts**: If something seems to be too good to be true, it probably is.

Trusted Resources

- Australian Cyber Security Centre (ACSC): https://www.cyber.gov.au/protect-yourself/staying-secure-online/connecting-others-online
- Farmers Guide to Social Media Safety: https://farmerhealth.org.au/2022/04/08/the-role-social-media-plays-in-creating-a-safer-healthier-agricultural-community
- Facebook Security: https://www.facebook.com/help/193677450678703

Thank You

https://www.csu.edu.au/research/farmers-cybersecurity