Protecting yourself online

1 Step 1: Privacy check up

Keep personal and professional accounts separate

- Consider using a different name on your personal and professional accounts – e.g. use a nickname on personal Facebook accounts.
- Remove personal details such as personal phone numbers and your home address from professional social media accounts and vice versa.

Check the privacy settings on your social media accounts

- Make sure your privacy settings are set to the level that you feel comfortable with. Consider setting your account to private or limiting who can see your posts. Complete a privacy check-up and security check-up on Facebook. Follow the safety guides for X (formerly Twitter, Instagram, Linkedin and TikTok.

Look yourself up online

- Google yourself and see where your name, phone number and address are listed online. You can request the removal of your data from data collection websites such as AeroLeads, Datanyze and Crunchbase.
- Check online CVs for personal phone numbers and home addresses.
- If you have a personal website registered under your name, look it up through whois-search.com. If your personal information is public, you can get domain privacy services from the company where you registered your domain name.

Review location settings

- Review location settings and posts on your social media accounts, including the tags and photos - e.g. a photo in front of a sold sign of your house could give away information about your location.
- Avoid 'checking in' to locations regularly so that others can't monitor your habits.

Review password security.

- Set up two-factor authentication.
- Check your account names/email addresses with Have I been pwned? Immediately change account passwords that may have been compromised in data breaches.
- Get a password manager or password keeper app – they are freely available in app stores. Look for the ones that are encrypted.

SCIENCE MEDIA SAVVY
ausSMC
Te Pōkai Tara Universities New Zealand
SMC NZ Science Media Centre

2 Step 2: Review your content

- Be mindful of what you post and how it may be interpreted. Avoid using inflammatory language and consider how your posts could be perceived.
- Google your subject area and play devil's advocate. Write down potential criticisms and how you could respond to these. They may be useful for responding to respected stakeholders, such as journalists, politicians or patients.
- Be honest and open about your work. Declare anything that could be perceived as a conflict of interest, such as your funding sources, commercial ties, or membership with campaign organisations.
- Talk to your organisation's media and communications team. They are experts in communicating.
- Find your digital allies. Speak to other high-profile academics in your area. They may have advice on subject-specific issues that can trigger online abuse.
- Be proactive. Have conversations with people who may be able to come to your aid.

3 Step 3: Have an action plan

Have a clear plan for what you will do if you experience online harassment. Suggested plans could include:

- Collect evidence. Take a screenshot or record the URL and handle of the account that posted the abuse.
- Have a plan to look after your wellbeing. Online abuse can cause real harm. A plan may include things you like doing (e.g. going for a walk), connecting with specific people (e.g. calling a friend), or things that bring you a sense of purpose and meaning.
- Report the abuse - Don't go it alone, tell someone. Report it to the platform, media outlet, Netsafe, to your work (this could include your line manager, the media team, IT department or the security department).
- Reduce notifications. Mute or block the account. Reduce your notifications to only those you follow. Ask colleagues to monitor your online content for you.
- Know what support is available to you through work and other avenues.

NOTE: Reach out to staff at your institution that respond to instances of online harassment proactively if you believe future research, funding announcements, media appearances and public engagement might attract negative attention.

This advice has been adapted from the Australian Broadcasting Company's Guide for Supporting External Talent.