Social Media protocols and procedures

Purpose

The purpose of this document is to outline the engagement protocols and procedures for AUSTRAC's official social media activity.

In applying these protocols and procedures, people should also be mindful of:

- IT Security policy obligations
- Complementary guidelines for AUSTRAC's people wishing to publish content through social media in a personal or unofficial capacity
- National Archives of Australia guidelines on social media record management.

Background

The term *social media* encompasses a number of tools that blend online technology and social interaction. Social media platforms provide opportunities for people to generate, share and exchange information in virtual communities and networks. Social media is also commonly referred to as Web 2.0.

Like other communication tools, these contribute to information dissemination as well as reputation management by working in complement with other communication channels. The use of social media is to be undertaken as part of a broader communication plan, which includes consideration of timing and the range of communication conduits used. Stakeholder Relations (particularly through Communications and Products) will take primary responsibility for developing communication planning.

Social media are distinguished from traditional or mass media channels because

- social media are interactive, conversational communication conduits rather than one-way modes
- social media platforms enable anyone to become a publisher, as opposed to a few major organisations which own telecast, broadcast or print media outlets
- social media are real-time, immediate and frequent forms of publishing, without technical production lead-times
- the readers of social media are visible and identifiable – in that participants need to set up accounts in order to take part – and their points of view are visible
- access is by personal computers and mobile devices such smart phones and tablets.

Social media is now widely accepted and used in the broader community. Increasingly, the public expect organisations to provide a forum which:

- broadcasts information about the organisation and its activities, publications and information
- provides a way for the public to respond and engage
- is succinct and prompt in its response.

Government context

These protocols have been developed with reference to the following:

- the government's *e-government and the digital economy policy* and *Digital Government agenda*
- Australian Public Service Commission (APSC) Circular 2012/1 *Revisions to the Commission's guidance on making public comment and participating online*

It is expected that Australian Government organisations will strive to listen to stakeholders and be responsive and approachable while maintaining the apolitical nature of the Australian Public Service (APS).

The APSC Circular (listed above) cites the APS Values and Codes of Conduct and these apply when using social media in the same way as when APS employees participate in any other public forum. The requirements include:

- behaving with respect and courtesy, and without harassment
- dealing appropriately with information, recognising that some information needs to remain confidential
- delivering services fairly, effectively, impartially and courteously to the Australian public
- being sensitive to the diversity of the Australian public
- taking reasonable steps to avoid conflicts of interest

- making proper use of Commonwealth resources
- upholding the APS Values, Employment Principles and the integrity and good reputation of the agency and the APS
- not acting in a way that would call into question the APS employee's ability to be apolitical, impartial and professional in the performance of their duties

Using Social Media

The objectives of AUSTRAC's official social media channels are to raise awareness, inform, engage, communicate with and learn from stakeholders and the Australian community. AUSTRAC will utilise two key social media channels. Others will be considered in due course, as opportunities suggest and resourcing allows.

Twitter

- Raise awareness of AUSTRAC's identity and areas of interest/operation
- Distribute links to media releases and other news, announcements, activities, event notices and updates
- Highlight and promote AUSTRAC activities, publications and other web-site content
- Address enquiries received via the channel
- Demonstrate connection with partner agencies and other stakeholders

Facebook

- Raise awareness of AUSTRAC's identity and areas of interest/operation
- Distribute media releases and other news, announcements, activities, event notices and updates
- Highlight and promote AUSTRAC activities
- Address enquiries received via the channel

Objective	Activity	Social media channel
1. Awareness Raise awareness of the agency and its purpose	Identify and follow partner agencies, industry associations and others of relevance to AUSTRAC's brand, areas of expertise and mandate. Post content linked to our areas of expertise and mandate. Re-tweet and share content, which is associated with our purpose, from partner agencies.	Twitter Facebook
2. Inform Distribute publicly-available information, in line with AUSTRAC's communication objectives	Post content and messages based on pre-approved material (e.g. from media releases, publications, existing web content). Co-ordinate timing and message consistency through Stakeholder Relations in liaison with relevant work areas.	Twitter Facebook
3. Engage Building relationships with key stakeholders or target audiences online	Identify social media accounts for stakeholders Where appropriate, 'follow' stakeholder accounts Re-tweet and share content, which is associated with our purpose, from partner agencies. Where appropriate strive to engage community members in a two-way conversation. Ensure that re-directs and responses are delivered promptly, especially if correcting inaccuracies or concerns.	Twitter Facebook

In due course, other social media channels can be assessed as appropriate. Each would be subject to the appropriate approvals prior to being activated. These could include:

YouTube

- Provides information in accessible video formats online
- All video clips require captioning

Linked-In

- A social media channel which can contribute to recruitment processes

Target audiences

Primary audiences

Stakeholders include those with an interest in, or a link to, AUSTRAC's strategic priorities and activities, such as partner agencies, industry associations, reporting entities.

Secondary audiences

- Members of the Australian community
- Attorney-General's Department and central agencies
- Mass media outlets and journalists who are conduits to reaching the Australian community
- Specialist media outlets that are conduits to the financial, compliance, risk management, national security, law enforcement and government policy sectors
- FATF membership

Unintended audiences

It is noted that, like all communications in the public domain, social media communications can reach audiences beyond those originally intended by AUSTRAC. It is accepted that organised crime groups, terrorist support groups and others are active in social media channels.

Developing a following

It is essential to develop a strong cohort of people/organisations following the social media channel. The value of a social media channel is driven by the size and breadth of the following.

This can be developed through the following practices:

- Sending follow requests to identified organisations and individuals with whom AUSTRAC has a relationship and shared interests.
- The expectation, as a social media courtesy, is that they will then follow in return. Accepting those follow requests is straightforward.
- As the network of followers expands, so does the pool of potential followers for AUSTRAC.
- Unsolicited requests to follow will be assessed on a case-by-case basis by reviewing the profile of the requester.

Branding

All social media accounts are subject to AUSTRAC's visual style guides. For advice and information on branding and the visual style guides, please review the guides on *OnTrac*.

Moderation

Authority

The person/s responsible for posting material on the official AUSTRAC social media channels will be authorised by the CEO. The nominated person will have the authority to post on the official AUSTRAC social media channels with oversight by their line manager.

In certain special circumstances, such as when an election is called and the Caretaker Conventions are evoked, AUSTRAC staff will notify the Executive regarding:

- any comments on social media that may require a response
- any postings on social media channels.

This will help to ensure that AUSTRAC's engagement, particularly during this time, will not be misconstrued as political comment.

Moderated accounts

All of AUSTRAC's social media accounts are moderated. This means that the sites are monitored for user-generated content and action taken where appropriate as set out below.

The nature of social media encourages discussion and engagement. The nature of AUSTRAC's work can lend itself to a broad range of perspectives and opinions.

The sites are monitored for content that might infringe privacy, impinge on security, disclose information of a threatening or harmful nature or is offensive, obscene, abusive, racist, sexist, homophobic, ageist, unrelated to the topic at hand, illegal or otherwise unhelpful to respectful and constructive dialogue.

Moderation procedure

1. The post will be hidden from public view, with notification provided to the user as a comment to their post.
2. This process should also be used when content is posted that discloses personal information about that user or anyone else.
3. Continual posts of inappropriate material will result in a post from the page as follows:
   "We've had to remove some posts from our wall that breach our moderation guidelines."
4. Posts where there is a threat or disclosure about the safety and wellbeing of a person require an immediate response. The situations for such posts cover the following:
   - Threat or disclosure of an act of terrorism
   - Dob-ins

In all of these circumstances, the moderator will respond as follows:

1. Urge the user to contact 000 if there is any immediate danger or if a serious incident has just occurred
2. Urge the user to contact the National Security Hotline 1800 1234 00 if the threat relates to an act of terrorism
3. Re-direct the user to the AUSTRAC Contact Centre if the matter relates to a dob-in or less immediate danger, and notify the Contact Centre of the contact received via social media.
4. All public posts in relation to these exchanges should be removed as soon as practicable, and after advising the user concerned where possible.

Monitoring and responses

Monitoring

AUSTRAC's official social media accounts will be monitored by a moderator in Communications and Products, on behalf of Stakeholder Relations, at 9.00am, 12.30pm and 3.00pm each business day.

AUSTRAC staff who regularly use social media are encouraged to notify Communications and Products by email if an urgent or important matter involving AUSTRAC is identified at other times. All AUSTRAC staff are

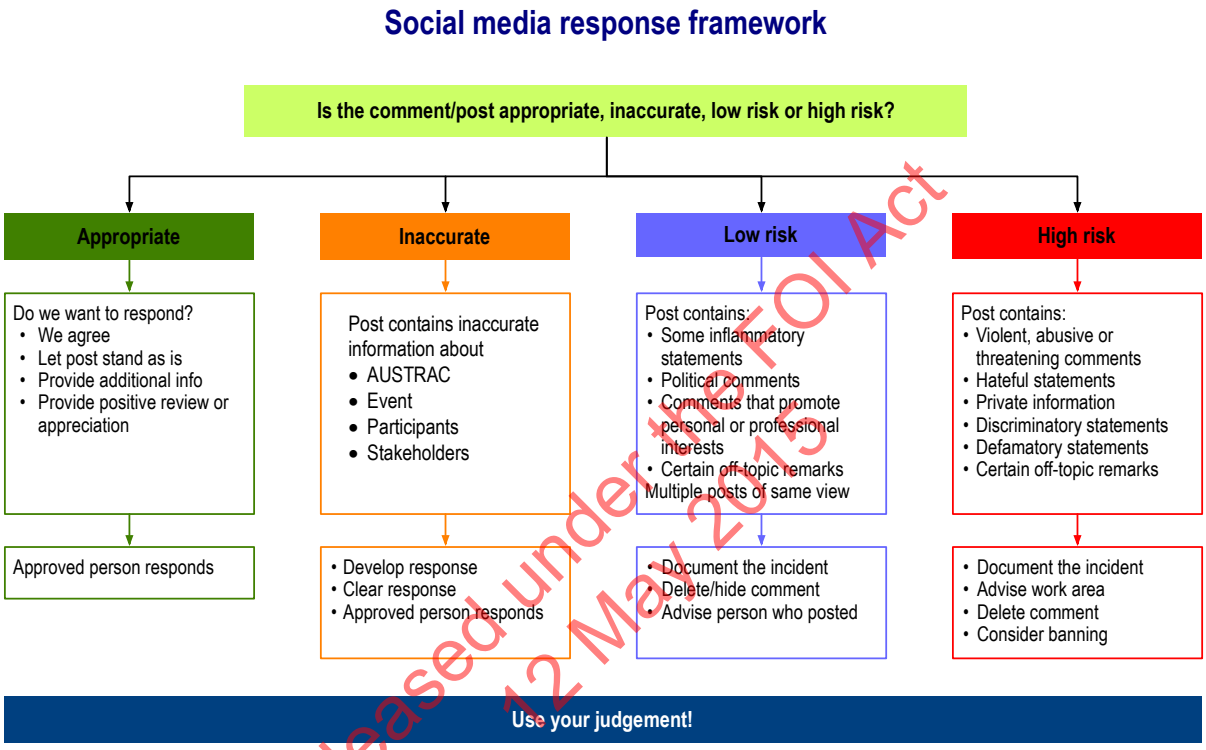
reminded that they are not to engage in the conversation on behalf of AUSTRAC. This can only be done through the official AUSTRAC channel.

Responses

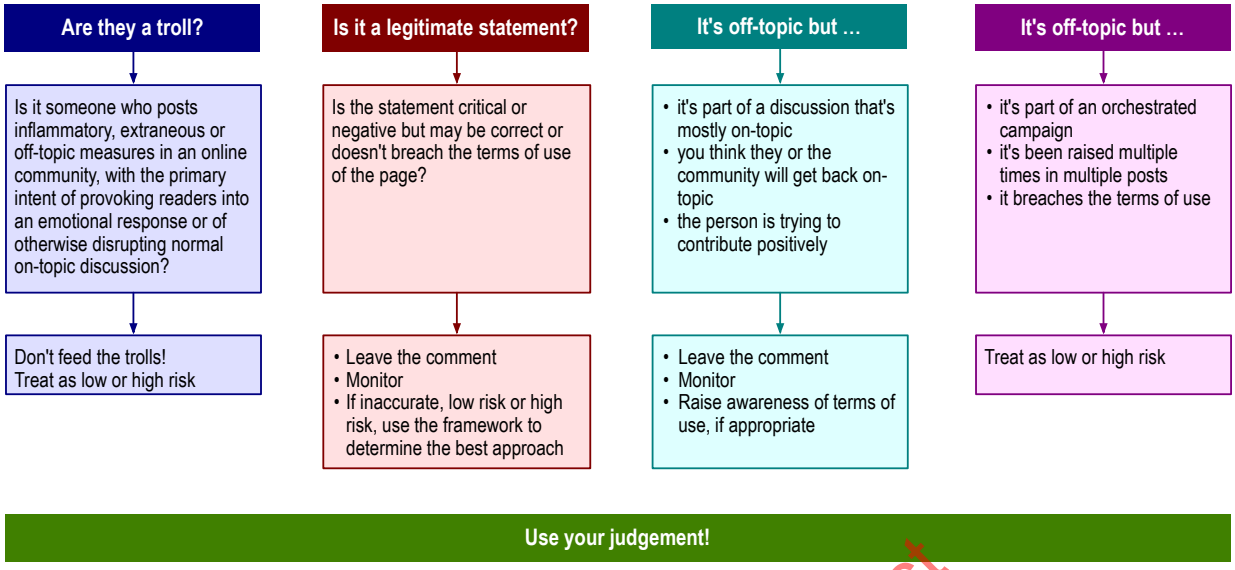
It is not essential to respond to every tweet or post. A few key considerations for assessing a post or tweet for a response include:

- is it directly related to our mandate
- is it accurate and/or positive about AUSTRAC
- is it a direct question (eg from an RE).

The flow diagrams, below, provide a decision frameworks for response types and for dealing with negative or off-topic posts or tweets.



Dealing with off-topic or negative comments



Style of expression

The content of messages, to be communicated via social media channels, will vary according to the nature and purpose of the communication. Posts will be factual and unclassified. Some key principles of language for the social media context are:

- a conversational tone is appropriate, while being mindful that the communication is emanating from an Australian Government body
- clear, concise language, using active voice is recommended
- effusive or emotional language should be avoided.

Stakeholder Relations (particularly through Communications and Products) will assist with suggested wording.

Use existing content

Where possible, responses to enquiries will be developed from publicly available information and direct the follower to the website or other publicly available source. Existing content in the public domain, such as on the website, is a valuable source of material.

A set of standard responses to common enquiries will be developed and maintained.

Some posts/tweets might best be handled by re-directing enquiries, such as an RE query might be re-directed to the Contact Centre.

Experience from other agencies indicates that it can be expected that 80% of the responses will be from pre-approved material while 20% will require a specifically developed response.

Developing a response

Where a specifically developed response is required, they will be handled in a similar way to approvals for publications, media relations, etc:

- responses developed with the relevant work unit
- cleared through Executive.

Due to the nature of social media, it is important to process these responses swiftly, in line with the following procedure:

1. The moderator of the social media account notes a post/tweet that requires a specifically developed response:
    a. notes the time of posting and receipt

b. acknowledges the receipt of the enquiry and undertakes to source an answer (e.g. “Interesting question. I’ll look into it for you.”)

2. The moderator contacts the relevant work unit to advise of the enquiry and works with the work unit to develop a draft response of the factual details in appropriate language tone and style.
3. The draft response is cleared with the relevant General Manager, then Executive General Manager, who will decide whether the CEO’s clearance is also needed. This decision will form the basis of attribution for the response.
4. When approved, the moderator posts the response on the social media platform where the issue was found, and notes the time.
    a. Responses to social media enquiries should be swift. The time between the moderator receiving the enquiry and posting the final response should be no longer than two hours.
5. The moderator must make a record of the interaction in the official AUSTRAC record keeping system (enquiry, approvals, response and timings) to ensure records and statistics of all social media interactions are recorded.
    a. This is in line with whole of Government requirements to create and manage accurate records of business activities so that decisions and actions can be accounted for; which includes the use of social media in an official capacity.

Evaluation

Communications and Products will conduct an evaluation of AUSTRAC official social media activity regularly to:

- monitor the uptake of the AUSTRAC social media activity among the primary and secondary target audiences
- monitor the nature of activity generated by AUSTRAC and followers
- identify any trends emerging from the activity
- evaluate the tone of behaviour on the various social media platforms
- compare AUSTRAC activity against the performance and experience of other agencies and learn from their use, including through involvement in the Cross Agency Social Media forum.

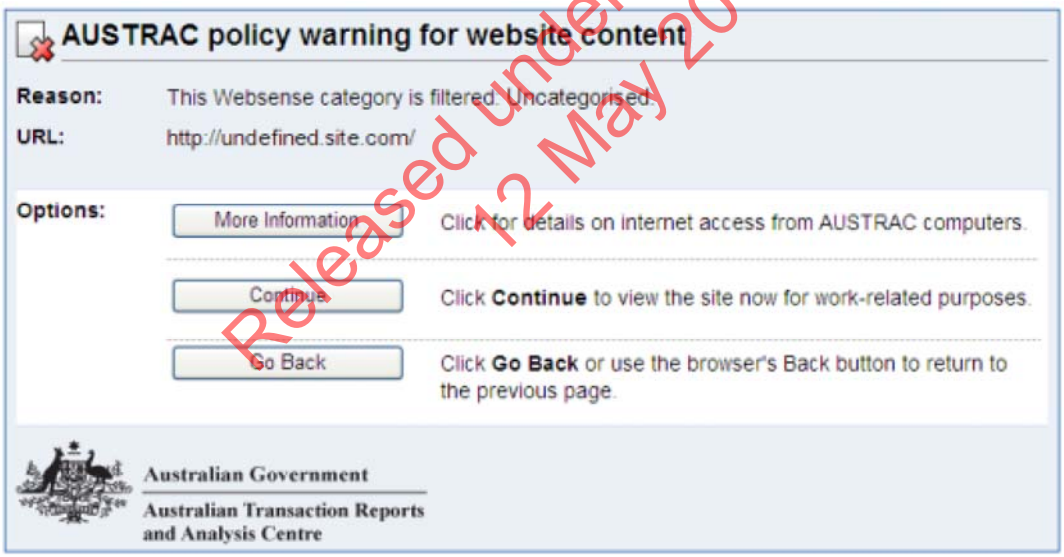
Internet access information

This page contains information on accessing the internet from AUSTRAC computers, supplementing the IT Security Policy [/node/1939/] and other documents.

Internet sites now outrank email as the most likely source of a computer virus or similar malicious software, and some pose significant threats to individual online privacy. AUSTRAC filters internet access in line with our policy and information security obligations.

Websites that display a policy reminder

Some websites are not completely blocked, but display a policy reminder when you try to access them. These are websites or categories that AUSTRAC considers are potentially unrelated to your work.



This is intended to remind you about reasonable and appropriate use of the internet in line with AUSTRAC policy. Read on below for explanation and examples to guide you on internet use.

The notification gives you three options:

1. Clicking the **More Information** button brings you to the intranet page you are reading now.
2. Click the **Continue** button if your use of the website is in line with policy. The website will then open as usual.

3. Click the **Go Back** button if you do not need to visit the site. For example, you may choose to access the site later from your home computer instead.

Websites that are blocked

If you attempt to access a website blocked by AUSTRAC, you will see this:

The **More Information** button links to this intranet page. The **Go Back** button returns you to your previous page. If you need to access a blocked site, contact the IT Service Desk to discuss the possible options.

Some categories blocked by AUSTRAC include:

- Malicious websites, which contain or link to code that may intentionally modify our computers without consent and to cause harm
- Counterfeit business sites aiming to eliciting financial or other private information from you
- Sites containing graphic adult content unsuitable for our workplace
- Sites that promote or support online gambling, illicit drugs, or criminal activity
- Sites that provide public webmail and similar online messaging services
- Sites that enable peer to peer file sharing and transfer
- Sites whose primary function is to provide freeware and software downloads.

AUSTRAC blocks these websites to reduce exposure to a range of risks. Blocked categories and individual sites are reviewed from time to time, and may change in response to factors such as AUSTRAC policy or new online threats. If you identify a website that should be blocked, but isn't, please alert the IT Service Desk [mailto:itservicedesk@austrac.gov.au].

Appropriate and professional use of internet access

All AUSTRAC staff (employees and contractors) are required to undertake their business and work relations in a professional and responsible manner. This is essential to protect AUSTRAC's professional image and the integrity of the information we hold.

The Australian Public Service (APS) Values and Code of Conduct set the standards of behaviour expected of public servants. Contractors, while not public servants, are also required (through their contracts) to adhere to these standards. Several elements of the Code of Conduct are particularly relevant to the appropriate and professional use of internet and emails:

- behaving with respect and courtesy, and without harassment
- making proper use of Commonwealth resources
- taking reasonable steps to avoid conflicts of interest
- at all times upholding the APS Values and the integrity and good reputation of the APS.

What does AUSTRAC expect?

Internet and email facilities are official resources provided by AUSTRAC to enable staff to carry out AUSTRAC business. In using these resources, AUSTRAC expects that:

- the information technology databases and systems, the internet and email will be used for official work purposes with limited personal use
- access to information is on a 'need to know' basis
- the security and integrity of the system and information will not be compromised, for example not observing password protocols and transmitting personal information without authorisation.

What is limited personal use?

AUSTRAC allows for staff to use the internet and email for personal use in limited circumstances. These may include internet banking and account payments or short, general information searches. It may also involve contact with colleagues and members of the public by email that is not work related. Any personal use:

- must not interfere with normal business activities (this includes both volume and content of private messages)
- must not have the potential to embarrass AUSTRAC, the APS or the government
- must not involve accessing inappropriate websites
- must not contain defamatory, offensive or harassing material
- must always maintain a professional tone
- must not be a means of bullying or causing distress or a sense of exclusion.

Some examples of inappropriate personal use include:

- frequent use of a social networking website throughout the day
- frequent visits to entertainment or sports websites
- extended or frequent periods of participation in a community discussion forum
- browsing websites idly without a specific purpose related to AUSTRAC work
- using your AUSTRAC email address to join or subscribe to online services that are not directly related to your work at AUSTRAC.

Does AUSTRAC monitor internet and email usage?

All internet activity and email traffic is logged, and those logs are retained under the

relevant legislation and regulations.

AUSTRAC routinely monitors access and usage, and this is a condition of using AUSTRAC computers. Monitoring is typically done for performance planning, troubleshooting, or security reasons. Periodic reports on internet and email use patterns are provided to management.

If there is reason to suspect misuse, an investigation may be conducted to determine whether there may have been a breach of the APS Code of Conduct or policy obligations. Breaches of IT, information management, protective security or personnel policies may result in loss or downgrade of security clearance, sanctions imposed under the APS Code of Conduct or in some cases criminal charges.

Where can I go for more information?

Questions about internet access can be directed via general request to the IT Service Desk [https://itservicedesk.hq.austrac.gov.au/HEAT] (call x0008 if urgent). Questions about IT Security policies should be directed to the IT Security Advisor [mailto:william.shipway@austrac.gov.au].

Alternatively, you may wish to speak to your manager, the Agency Security Advisor or the Director, Employment Conditions and Services.

This page is maintained by the IT Security Advisor [/users/wshipway] and feedback is welcome [mailto:william.shipway@austrac.gov.au].

Related information

Please be mindful of IT Security Policy when accessing the internet.

- APS Values and Code of Conduct [http://www.apsc.gov.au/aps-employment-policy-and-advice/aps-values-and-code-of-conduct]- including guidance for making public comment and particpating online
- AUSTRAC IT Security media watch [http://ontrac/blog?term_node_tid_depth=130&created_1=&created=]
- Social Networking: Privacy and Safety [/node/3306/]- an IT Security quick reference guide
- Stay Smart Online [http://www.staysmartonline.gov.au/]- protect yourself
- CyberSmart [http://www.cybersmart.gov.au/]- advice for parents, teens and kids

Social networking: privacy and safety

AUSTRAC computers and internet access are Commonwealth resources, to be used for work purposes in line with our policies. However, AUSTRAC staff and contractors may choose to use social networking tools in their own time using their own resources. This sheet provides privacy and safety advice.

Your relationship with AUSTRAC

Any personal or professional use of social media by AUSTRAC staff and contractors must not bring AUSTRAC into disrepute, imply AUSTRAC endorsement of personal views, compromise effectiveness at work, or disclose official information. If a site requires your employer, list Australian Government in preference to AUSTRAC, due to the sensitivity of our work and the dangers of becoming the focus of undesirable attention.

Guard your personal information and reputation

Social networking sites like Facebook require you to submit personal information about yourself, and sometimes about other people. These sites may have options to control the information you share with others, and options to manage interaction with other people. Be very selective with what information you put online, how you share it, and who you accept as a 'friend'.
Some people use social networking sites to threaten, harass or embarrass others. Criminals actively use these sites to access personal information and steal identities. Criminals also use personal information for other illegal activities in the real word, and you can be unknowingly targeted or implicated.

Protective steps for social network sites

The following page lists important steps that can help protect you, your family, and your friends. These steps also protect your colleagues, your work at AUSTRAC and the sensitive information we are required to safeguard.

- Always type your social networking website address into your browser or use a bookmark. Links shown in emails or on websites can be very easily manipulated, sending you to malicious sites. Forged emails are common.
- Use a different password for each social networking site. When one password is leaked (it will happen), your other accounts should be safe.
- Protect your accounts with strong passwords, and enable extra account protection if offered. Eg enable an SMS token or authentication app.

- Set your online profile to 'private' and be very discerning about who you accept as your 'friend'. If you haven't met in person, you don't really know them. Online identities can also be faked very easily.
- Think before you post – expect many people other than your friends will see what you put online, now and years in the future. It's virtually impossible to remove content completely, once it is available online.
- Don't post information that would make you or your family vulnerable, such as date of birth, home address, the detail of your daily routine, child's school, or holiday plans. Yes, burglars do know how to use the internet.
- Don't post photos or details of family, friends or colleagues that may be inappropriate, or that they haven't agreed to being posted. Turn on Facebook's review option, to approve others 'tagging' you in their photos.
- Be alert to suspicious links and out-of-character messages or posts. Even if received from your friends, they may have had their account hijacked.
- Familiarise yourself with scamwatch.gov.au and common types of fraud. The internet and social media are regularly used for scams.
- Avoid using social networking from public or shared computers. Even if you log out, keystrokes or personal details may have been captured.

Where can you go for help?

Concerned about:	Contact:
Harassment or bullying online, or someone who is at risk?	See the ThinkUKnow [http://www.thinkuknow.org.au/site/] and Cybersmart [http://www.cybersmart.gov.au/] sites for advice, or contact the AUSTRAC PSS team
Fraudulent use of your identity or other criminal activity?	Your social network provider, and if appropriate, your local police or CrimeStoppers on 1800 333 000
Your online security at work?	AUSTRAC IT Help Desk, or AUSTRAC IT Security Adviser [mailto:itsa@austrac.gov.au]
Your personal safety?	AUSTRAC Protective Security [http://ontrac/security-and-emergency/security/protective-security-2071]