Cyberstalking: Behaviours, prevention measures and response options

Cyberstalking refers to an existing behaviour (stalking) using new media (information and communication technologies; Ogilvie 2000). Moriarty and Freiberger (2008: 137) analysed newspaper accounts of cyberstalking incidents and found that 54 percent of the alleged offenders fit a ‘domestic violence’ typology, ‘motivated by the need to establish, continue or re-establish the domestic relationship, where he/she could have or maintain control over the victim’. A further 15 percent were classified as ‘erotomania/delusional’ offenders, ‘motivated by the stalker’s fixation with someone he or she cannot have’. The remaining 31 percent were ‘nuisance’ offenders, ‘in this type of stalking, the victim is targeted and continually harassed by the stalker’.

The behaviours exhibited in the sample included:
» threatening, harassing or obscene emails (32%);
» live chat harassment or flaming (online verbal abuse; 19%);
» leaving improper messages on message boards or in guest books (11%);
» sending unwanted instant messages that instil fear or cause harm (3%);
» sending unsolicited email (1%);
» tracing another’s computer or internet activity (2%);
» electronic identity theft or unauthorised use of a website (4%);
» threatening, harassing, or obscene telephone calls placed to a cellular telephone (15%);
» sending threatening, harassing or obscene text messages to a cellular telephone (5%); and
» tracking a person’s whereabouts using a GPS without the person’s knowledge or consent (4%).

Reyns (2010: 110–111) outlines situational crime prevention methods for cyberstalking that can be implemented by individuals and ‘place managers’ (e.g. website administrators, webmasters and web designers) on a variety of forums, including email, blogs, social networking sites, message boards and forums, online dating sites, instant messengers, text messages, video messages and chat rooms. Prevention methods for individuals include:
» making email addresses unavailable or increasing the effort required to obtain them;
» using spam filters;
» not replying to cyberstalkers;
» limiting access to sites;
» limiting exposure, such as not posting personal information or photos;
» changing their online identity if necessary;
» not accepting messages from unknown parties; and
» avoiding problem sites.

Prevention methods for place managers include:
» making email addresses unavailable or increasing the effort required to obtain them;
» embedding personal identifiers into sent emails;
» monitoring sites and public boards for misuse;
» providing a clear code of conduct and reminders for users;
» increasing the effort required to obtain an account;

Contact Us
Providing crime prevention policy makers and practitioners with evidence-based resources and training to prevent and reduce crime.
www.cpassist.aic.gov.au

ISSN 1448-1383
» restricting access of accounts to ‘friends’ only; and
» enhancing surveillance by providing more ways to report abuse and unwanted contact.

There are a number of response options for those that are being cyberstalked, including:
» blocking unwanted messages;
» reporting to site administrators;
» talking with friends and family and/or making use of support helplines such as Lifeline (phone 13 11 14);
» keeping evidence such as taking screenshots or printing offending pages and messages; and
» reporting to the state or territory police (particularly if there has been a threat to safety).

NEED TO KNOW MORE?
All URLs correct at May 2013