# Domestic Violence and Technology

*This fact sheet summarises the Ask LOIS webinar on this topic, presented by* Charissa Sun, Solicitor, Women's Legal Services NSW *on 3 September 2013. This webinar can be downloaded for free at* [www.asklois.org.au/webinars/past-webinars](www.asklois.org.au/webinars/past-webinars).

**This fact sheet covers:**

- Cyber safety
- Digital footprint
- Account access / takeovers
- Social engineering
- Spyware
- Mobile phones & computers

## Cyber Safety

Perpetrators can and do use technology to perpetrate abuse:

- **Cyberbullying -** writing nasty comments, posting embarrassing pictures, spreading false or misleading information about the victim on the Internet

- **Cyberstalking** - using technology to harass, threaten or frighten

- **Digitally Assisted Stalking** - stalking activity which is enhanced or accelerated by the use of technology (such as mobile phones, computers, the Internet and spyware)

## Digital Footprint

- Information you leave behind – everything you do online leaves a trace
- Information other people leave behind about you
- **Risks**
    - Gives stalkers the information that feeds their obsession
    - Information used by perpetrators to help them intimidate, humiliate, or harass
    - *E.g. Online information can be used to establish a pattern of where we go, who we know, how we are feeling, our specific location, etc*
- **Technology Safety Planning**
    - **Assess what online information exists about you**
        - Do a Google search of yourself to see what information is available online so you know what precautions to take.
    - **Online accounts with profiles or an online presence**
        - Change your email and passwords
        - Delete existing online accounts, particularly it they contain large amounts of information or photos (eg Facebook, Instagram, etc)
        - Delete entries and photos
        - Review who can access your information
    - **Review all the privacy <u>and</u> security settings**
        - Highest possible privacy settings and security settings
    - **Avoid public forums**
        - Perpetrator can see your posts
        - Avenue of bullying and harassment

## Account access | Takeover

- **Account access -** when someone gains access to another person's account without their permission
- **Account takeover -** when someone accesses another person's account and then changes the username or password so that the original account holder can no longer access their own account
  - Perpetrator either knows or can guess the victim's username and password
  - Change passwords and update email addresses on all accounts

**Risks**

- Physical harm
- Financial loss (through accessing online bank accounts)
- Harassment, humiliation, abuse of victim
- Damage or destruction of victim's relationships by accessing victim's email account to send family, friends, work colleagues or clients abusive messages or messages telling them to never contact the victim
- Perpetrator can use the victim's account to send themselves abusive messages in order to incriminate the victim

## Social Engineering

- When a perpetrator manipulates someone to divulge confidential information about the victim
- Stalkers often use social engineering to gather information about the victims – finding out where they are, their new phone number, email, address, where they work, if they are seeing someone new
- Stalkers use information available online (digital footprint) to manipulate others into providing further information about the victim.
- *Article: Hacking the Mind: How & Why Social Engineering Works*

*http://www.veracode.com/blog/2013/03/hacking-the-mind-how-why-social-engineering-works/*

**Risks**

- Physical danger / access to victim
- Data gathering
- Harassment, humiliation, abuse of victim
- Installing spyware
- Account access / takeover
- Identity theft

**Technology Safety Planning**

- Clean up the computer – remove spyware
- Change all passwords and PIN numbers
- Limit what you share online
- Educate family, friends and work colleagues

## Spyware

- Apps or software that can be download onto a person's mobile phone or computer to collect information about them
- Monitors their movements, phone calls, text messages, etc.
- Tracks everything that the person does without their knowledge and sends the information to a third party
  - Mobile phones
    - Example: **mSpy** – smartphone monitoring software

- ‘Listens’ to and records conversations between people who are not on the phone – ‘remote listening device that will spy on its owner’ – records sounds within 4 ½ metres of the phone and is completely invisible on the target phone

- Computers
  - **How does computer spyware get uploaded?**
  - The perpetrator sends a victim an email that has a file attached – picture, PDF or other document, etc.
  - When the victim opens the file the spyware is downloaded in the background without the victim knowing.
  - **What computer spyware can do:**
    - Log key strokes
    - Captures all instant messaging (IM) chat conversations
    - Shows all websites visited
    - Monitors what is written online and in social networks
    - Reads your email
    - Shows your usernames and passwords
    - Captures screenshots of what you are doing on your computer
    - Allows third party to control your computer – e.g. launch programs, upload or download files, turn on the computer’s webcam and microphone
    - Example: **SniperSpy** – remote monitoring software
      - Can be remotely installed/uninstalled on a computer
      - Records user activities and sends it to an online account
      - View live screenshots and live keystrokes
      - Check Facebook and other social media activities

**Technology Safety Planning**

- Requires an internet connection to function – disconnect your computer or mobile phone from the internet
- Factory reset the computer or mobile phone
- Use spyware removal software
- Be extremely careful about opening .exe files
- Do not open attachments, pictures, cartoons
- *Article: How to detect if you are being monitored on your mobile phone:*

*http://acisni.com/is-there-spy-software-on-my-cell-phone-how-to-detect-being-monitored/*

## Mobile Phones

- Smartphones can increase the risk for DV survivors and stalking victims because they contain **sensitive information** and have **apps that leak data about us**. E.g., it can lead people to our exact location
- User information stored on the phone is also stored on the Internet through **Google** or **iCloud**
- Important for victims to **secure both** their **mobile phones** and its **associated online content**
- User information and data stored on Android phones or iPhones link to an online account. The online account store contacts, calendars, photos, documents, apps, etc.
- Can show the phone/user’s location, e.g. iPhone built in ‘Find your phone’ app

**Risks**

- Physical danger / access to victim / account access / takeover
- Financial loss - iCloud and Google allow users to store their credit card details online so that they can download paid content. A perpetrator can maliciously download content and run up a big bill. Or they can add a device to the online account and download paid content for their own use
- Data gathering – invasion of privacy, feeds obsessive behaviour

**Technology Safety Planning**

- Secure your Google or iCloud account
- Immediately change your login details for your mobile phone account – choose secure password that perpetrator will not be able to guess
- Delete apps that you do not use
- Review apps to see if they have any features that could be used to give away your location or leak information about you

## Computers

- **Internet Browsers –** a program used to access the internet and view webpages
- **Browsing history** – some browsers, for example, Chrome (Incognito) and Internet Explorer (InPrivate) allow for 'private browsing' that does not log your web history of the pages you visit
- Be careful as information can be synced across the same browser on different devices
    - *Article: How to Sync Your Browser Data in Any Browser and Access it Anywhere* *http://www.howtogeek.com/139179/how-to-sync-your-browser-data-in-any-browser-and-access-it-anywhere/*
- Be aware that in Firefox browser all saved usernames and passwords **can be accessed and viewed**
- Do not save your password and user information in the browser. Do not tick 'Remember my password on this computer' when at risk

## Resources

- **Network for Surviving Stalking**
    - http://www.nssadvice.org
- **Digital-Stalking | *Self-help to stalking***
    - www.digital-stalking.com
    - Victims Advice – Internet, Social Networks & Mobile
        i. http://www.digital-stalking.com/digital/
    - Publication: Digital stalking: A guide to technology risks for victims (version 2, Nov 2012), Jennifer Perry
- **Cyber(smart:)**
    - Glossary: http://www.cybersmart.gov.au/glossary.aspx#C