

No-one need live in fear

Southern Domestic Violence Action Group

PO Box 437, Noarlunga Centre
Ph:(08) 8384 9555
Fax:(08) 8384 9557

Taking and reporting on action against violence is at the heart of the Southern DVAG as the following pages attest....

<http://southerndvag.com/>

Issue 33:
Winter 2013



Southern Domestic Violence Action Group (SDVAG)

Meets 2nd Wednesday of every month

Next Meeting at Family & Relationships Centre
38 Beach Rd
Christies Beach
Meet at front reception

From 10am – 12:30pm

TECHNOLOGY SAFETY

What is High Tech Stalking?

Stalkers are increasingly misusing a variety of telephone, surveillance, and computer technologies to harass, terrify, intimidate, coerce, and monitor former and current intimate partners.

Stalkers may misuse technology to:

- Send multiple emails or text messages a day
- Monitor a victim's computer activity through Spyware
- Track the location of a victim's vehicle using GPS
- Watch the victim through hidden cameras
- Intercept phone calls and messages
- Impersonate the victim to cause harm

In most cases, a stalker will misuse multiple technologies at once while also using more traditional, non technology tactics.

Why is High Tech Stalking Important ?

As technology has become a major part of our everyday lives, it has also become more common for stalkers to misuse these new resources. It is important for all services and agencies who are working with victims of stalking to understand these technologies, how stalkers misuse them, and what strategies victims can use to increase their safe



Welcome to the Winter Issue of the Southern Domestic Violence Action Group's

STOP
VIOLENCE
AGAINST
WOMEN

Inside this issue...

- Technology Safety
- Reclaiming Safety
- Online Privacy Tips
- Posting Online Content
- Tech Savvy Teens
- Who sees your info,
- Spying on you

How Will You Know That Technology is Involved?

In most cases, victims know that some technology is being used and will report that the stalker "knows too much" about their computer activity, places they went to, their day today activities, and conversations they had on the phone. It's important that agencies and services trust a victim's instincts and help explore what technologies the stalker may be u



No-One Need Live In Fear – Winter 2013

Thank you to all who contributed to the issue and Amanda Rishworth, MP (Member for Kingston) for the printing.

Reclaiming Safety



What Can Agencies and Services Do?

- Agencies will be in a position to help victims safety plan around the misuse of technology. Because high tech stalking can provide the stalker with sensitive information and the victim's location, it's crucial that technology be included in safety plans to decrease risks.
- In many cases, agencies can also advocate with or for victims with mobile phone carriers and other companies, like online social networking sites, to help make changes to the victim's account or remove information from a website. (In these cases, a confidentiality release may be needed).
- Agencies and services can also help victims document the tactics that the stalker is using and the events the victim is experiencing so that a record is made. If the victim chooses to report the stalking to the police this documentation can be used to help begin a stalking investigation

Online Privacy & Safety Tips

Browsing the web safely and privately is concern for many people. A good general rule is that nothing online is private. Another general rule is that you can't be completely anonymous online. However, you can take steps to prevent sensitive and personal information from making its rounds on the Web.

Email

- Have more than one email account and use them for different purposes.
- Create email addresses that don't contain your full name since that can be very identifying.

Passwords

- Safest passwords contain letters, numbers and symbols. Avoid words that are in a dictionary and any important dates.
- Try not to have the same password for every account. Come up with a system that's easy to remember but will enable you to have a different password for each account.

Social Networks

- Check out the privacy settings and make sure it's set to the level of privacy you want. . Keep in mind that even if you set your social network page to private, it doesn't guarantee that your information is completely private.
- Don't forget that your friends may be able to see your other friends' posts and pages even if they're not friends with each other.
- Be thoughtful about who's on your friend list when you post or link to certain things.
- Read the social network's privacy policy and find out who else has access to your information, such as advertisers, third parties, etc.

Online Accounts

- Read the privacy policy. When you create an online account, whether it's to buy things, to join a group, or open an account, you should know what that site does with the information.
- Pay attention when creating an account. Oftentimes, this is when you can opt out of sharing personal information beyond what's necessary to create an account.
- Click "no" when it offers to check your email address book to find your "friends." Some illegitimate sites have used this option by sending spam and viruses to everyone in your address book.

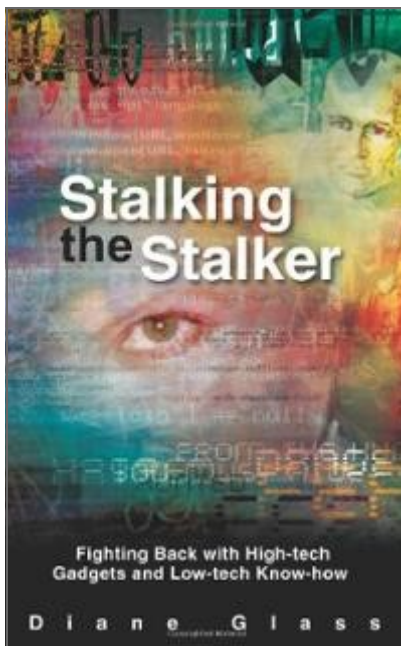


High Tech Stalking

Online Privacy & Safety Tips

Online Accounts (Cont. from p. 2)

- Try not to use your name or a combination of your name as your username.
- When filling out account profiles, for increased privacy give none or very minimal information and opt out of joining the site's directory.
- For more privacy, try not to use too many applications with one account username/password. If someone guesses your username or password, they'll have access to all your applications.
- Log off when you're not using an account and do not choose to have the computer remember your passwords.



Friends & Family

- Talk to your friends and family about what they can post online about you.
- Don't forget that employers, churches, sport teams, groups and volunteer organizations that you are a part of may share your personal information online.

Safe Web Browsing

- Make sure you are running antivirus and antispyware software and make sure that definitions are updated.
- Periodically run scans on your computer, separate from your regular antivirus/antispyware, such as bitdefender online scanner : <http://www.bitdefender.com/scanner/online/free.html>
- Periodically delete history, cookies, temporary internet files, and saved forms and passwords from your web browser.
- For added privacy, use a proxy server when you browse the web.
- Most search engines keep records of search terms, so when using search engines, avoid

Telstra Help for Domestic Violence Victims.

Telstra has put in place a new program to provide a concession for eligible Telstra customers facing a personal safety threat due to risk of domestic violence who require a Silent Line service on their home phone. Telstra's silent line service stops their name, home phone number and address from being listed in White Page Directories or being given out by Directory Services. It also stops their number from being displayed on Calling Number Display when calling others. Usual cost for Silent Phone Number feature is \$2.93 but Telstra will provide an exemption if you meet their criteria. Public information about this program is available at www.telstra.com.au/accessforeveryone Or call Telstra Consumer Affairs on 1800 804 591.



No-One Need Live In Fear—The Purple Booklet, Edition 6, 2013..Domestic Violence Information & Resources. Available from Southern Women's on 8384 9555.

SOUTHERN DVAG

We would like to invite you to attend our Annual General Meeting.

DATE: Wednesday 11th September, 2013

WHERE: Port Noarlunga Football Club
Britain Drive, Port Noarlunga

TIME: 10 am to 12.30pm

SPEAKER: Michelle Jardorn- "Research and Resistance:
A Cautionary Tale"

RSVOP by 6th Sept. Transport is available. Call 8384 9555



High Tech Stalking

Privacy Considerations When Posting Content Online

The Internet is full of opportunities for us to share things about ourselves, whether it's a blog entry, updating our Facebook or MySpace status, or posting videos on sites like YouTube. We post information to share our lives with our friends and family, but this information also becomes viewable by millions of other people as well. Some people may not care that the things they share about themselves can be viewed by anyone, but other people. For those who want to be more protective of their online information, here are some questions to consider when posting content online.

Who Will See This Information?

Sometimes we don't realise how far and wide our information is shared; especially when we think we're just posting updates about ourselves to our friends.

With the Internet and search engines (like Google, Yahoo!, Bing and others), everything online is indexed and searchable. Even sites where you think only members can see the content could be public or seen by others who aren't members, anywhere in the world.

What Are You Sharing?

From a privacy perspective, the kind of information you share can reveal a lot or very little about you. Sometimes we share personal information about picture or even blogging about a great restaurant can indicate where you are or have been. Consider if what's okay for others to know. Are you sharing information about others, and if so, do you have their permission? Be careful when sharing information about your friends and family because you may reveal something that they don't wish others to know.

What Is the Site's Privacy Policy?

Do you know what the owners of the website do with the information you give them? Even if the information you share isn't posted online, it may be shared with advertisers or third parties. Many sites have privacy policies that spell out what they do with the information you give them.

Is the Information You Share Illegal or Against the Content Policies of the Site?

If you want to share information online, make sure you comply with laws (such as copyright and fair use, etc.) and with site policies. Many sites do not allow violent or discriminatory content; some sites will remove "banned" content or even close the related account. Sometimes, posting false information, harassing or harmful content can even result in civil or criminal legal action. If you aren't sure, find out about the relevant laws and policies first, before you post.

How Much Control Do You Have Over The Information That You Share?

Some people believe that because it's content you posted, you own it and can control it. However, you really don't have much control because once it's out there, others can share it, talk about it, and even change it. If you originally posted it on your personal website, blog, or social network page, you could take down the original post. However, it will likely be difficult for you to have it removed once it's on



What can I do to increase my privacy?

- Be thoughtful about what you share online.
- Be careful about what you post about other people.
- When creating online accounts read the instructions carefully. Oftentimes this is when you can opt out of the site owners collecting and sharing your information.



Tech Savvy Teens

Choosing who gets to see your Info

BLOGS AND SOCIAL NETWORKING

Have you put your Blog on a Social Networking Site like Facebook or My Space or an Online Dating Site? Have you set your Profile to be Private? If not, anyone who visits that site, including University admissions officers, teachers, family, potential employers or even stalkers can see your personal information.

Do you use Free email, a blog, instant Messaging, or share music or photos online? When you signed up for that service, did you give your name, age, gender, the town you live in or your hobbies? If, so, the company that got that information might post it online for everyone to see. Many times, you can choose not to have your information included in public directories. You can also provide very little information if you want (only your first name or a fake name, for example).

Have you ever sung in a school choir, had your work included in an art show, or been in a sports team? If so, your name, personal details, and contact information might be posted online. Some websites will remove information at your request, but the site is archived, your information may not really be gone. If you don't want information posted online, you should act quickly to have it removed.

Archives Websites can be “archived” or “cached” so people can still access the old content even if the website disappears or changes. This means that any information posted to the Web could be online for a long time – maybe even for ever. Internet Archive (www.archive.org) has 55 billion webpages.

Other Ways Your Information Gets on The Web

- A Store asks for your phone number or postcode when you buy something and that information is put on a database. The online store might later sell your information to a data broker who posts it to an online directory.
- A friend or classmate posts information or photos that include you. Or, a relative posts a family photo album with you in it.

Removing Information Sometimes it's okay to leave certain information online, especially when it is harmless. When trying to remove any information from a website, consider not sharing your correct information because data brokers make money by selling accurate information. If you want something removed, the website may have instructions,, or provide a form or email address to contact them. If the information is a government record, you may need to fill out an official request or write a letter.

How do I know what is on the web already? **If you can find it, someone else can too!**

- Search the web for your personal information and photos. Some places to start: Google, Yahoo, Facebook, You tube and Flickr.
- Look on websites for groups and places where you might have a connection: your school , clubs, jobs, religious community, sports teams, community and volunteer groups, etc.

Are you receiving hundreds of text messages or voice mails from someone you don't want to talk to? For support, you can call Kids Helpline 1800 551 800,. You can talk to your phone service provider about call blocking , or about changing your number. You can talk to the police to find out if there is evidence for a stalking or harassment charge. Harassing phone calls are often illegal.





Spying on you

Does someone seem to know about every email you have written or everything you wrote in an Instant Message? People can log into your instant messaging or change your email account settings so they can see copies of your emails. Stalkers can install spyware or hack into your computer. Attachments are notorious. If you think there may be spyware on your computer, use a library or friends computer. Use another computer to change your password.

If an abuser has access to your email or instant messaging, use another computer to create a new email account. Look for free web-based email accounts and don't use identifying information in your new email. (eg. Use bluecat@mail.com, not yourname@mail.com). Read the registrations and choose not to be identified in any directories.

Stalkers can put spyware on mobile phones, so change your password often and use a combination of letters and numbers.

Emergency Numbers

Emergency: 000

Police: 131 444

DV Helpline: 1800 800 098

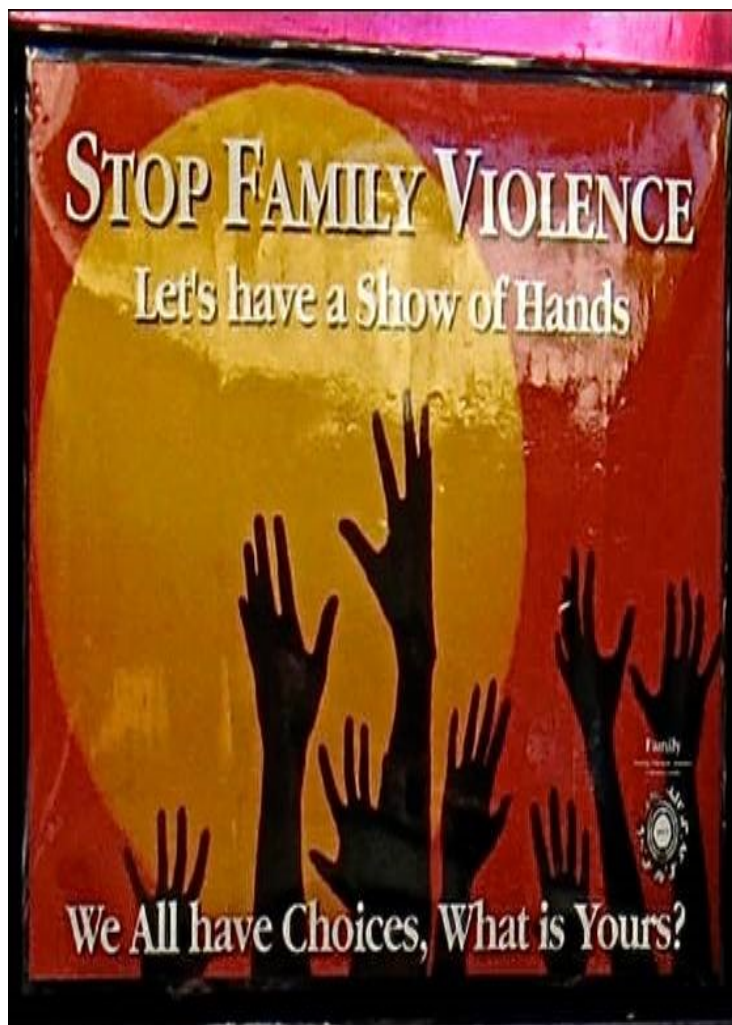
DV Crisis Service : 1300 782 200

Crisis Care weekends, nights:
131 611

Kids Helpline: 1800 551 800

Crisis Care: 131 611

Child & Youth Health Parent Helpline: 8303 1555



Thank you to the SDVAG for contributions to this newsletter. For more information or to provide feedback please phone 8384 9555



Membership

ABN: 33 467 685 846

☐

New member

☐

Renewal

Membership is renewable annually

Name: _____

Organisation: _____

Address: _____

Phone: _____

Mobile: _____

Email: _____

Email me my newsletters

☐

Confidentiality

I may be contacted by phone

☐

I may be contacted by mail

☐

No contact whatsoever please

☐

Community membership

\$5

☐

Organisational membership

\$30

☐

Donation

\$ _____

Cheques or money orders can be made payable to Southern Domestic Violence Action Group Inc. This form becomes a tax invoice when you make your payment. Donations of \$2 or more are tax deductible.