

Digital stalking:

A guide to technology
risks for victims

Jennifer Perry

Published jointly by Network for Surviving Stalking and Women's Aid Federation of England.

With grateful thanks to Nominet Trust for funding the development and writing of this guidance, and to Avon UK for supporting its publication.

Network for Surviving Stalking

PO Box 88
Lydney
GL15 9AG
Telephone: 07501 752741
E-mail: info@nss.org.uk
Website: www.nss.org.uk

Women's Aid

PO Box 391
Bristol
BS99 7WS
Telephone: 0117 944 4411
Fax: 0117 9241703
E-mail: info@womensaid.org.uk
Websites: www.womensaid.org.uk www.thehideout.org.uk
0808 2000 247: National Domestic Violence Helpline (run in partnership between Women's Aid and Refuge)

© Network for Surviving Stalking and Women's Aid Federation of England, 2012
ISBN: 978 0 907817 52 9

Author: Jennifer Perry

Jennifer Perry is an internet safety expert and consumer advocate. She wrote the first UK *Internet Safety Guide for Survivors of Domestic Violence and Stalking* in 2008. She works with a wide range of stakeholders including: government, enforcement agencies, industry groups, security and legal experts as well as support charities. This gives her access to the latest thinking on e-crime and anti-social issues facing internet users. Using this collaborative work, she translates 'tech speak' into clear, easy to use information for consumers, helping them to resolve their problems and avoid becoming an online victim. She helps organisations to develop their online safety strategies, support and policies. She provides training on social networks, online harassment/stalking and reducing online risks.

Jennifer was founder of E-Victims.Org a charity that helped victims of online crime in 2006. She helped over 3,000 victims and had over 100,000 visitors to the website. The charity ceased operations in September 2010. Jennifer worked for 20 years in senior marketing roles for consumer technology companies first in the computer and then in the internet industry. Her role was to engage consumers in technology by helping them understand it and making information user friendly.

Production Editor: Susannah Marwood

Contents

Acknowledgements	4
Foreword	5
Preface	6
Digital stalking: a guide to technology risks for victims	
Introduction	8
Digital footprint	11
Social engineering	13
Mobile	16
Geolocation	20
Computer monitoring/spyware	24
Social networking	27
Account access/takeovers	31
GPS devices for a car	34
Spoof SMS	35
Survivors of domestic and sexual violence	36
Stalking in the workplace	40
Appendix A: Warning signs of a stalker	42
Appendix B: Key actions to reduce cyberstalking risks	44
Appendix C: Gathering evidence	46
Appendix D: Password security tips	48
Appendix E: E-mail – creating new accounts	51
Appendix F: Share cautiously	53
Appendix G: Social networks – safety tips for stalking victims	54
Appendix H: How to set Facebook's privacy settings to increase security	55
Appendix I: Disabling mobile pictures' geotags	58
Appendix J: Security tools for victims	61
Appendix K: Support organisations	63
Technology glossary	64
Bibliography	69

Acknowledgements

The author wishes to express sincere appreciation to Wendy Green and Karen Evans for providing their invaluable insight and encouragement into this project. The following individuals and organisations also generously shared their expertise and time:

Charlotte Aynsley, Beat Bullying
David Benford, Blackstage Forensics
John Carr, Online Child Safety Consultant
Dr Richard Clayton, Cambridge University
Graham Cluely, Sophos
Karen Evans, North East Hampshire
Domestic Violence Forum
Neville Evans, Author/talkandsupport.co.uk
Wendy Green, Rushcliffe Borough Council
Nicola Harwin, Women's Aid
Mike Hawkes, Mobile Data Association
Dr David Holmes, Manchester Metropolitan
University
Martin Hoskins, T-Mobile and Orange

Anthony House, Google
Professor Carsten Maple, University of
Bedfordshire
Ibby Neville, Mobile Forensic Specialist
Roland Perry, Internet Policy Ltd
Larry Pesce, ICanStalkU.com
Tim Snape, South West Internet
Dr Emma Short, University of Bedfordshire
Kristiana Wrixon, National Stalking Helpline
Facebook
Internet Service Providers Association
Kaspersky Lab
Microsoft, Essentials Security Team

Foreword



At the beginning of 2011, Jennifer Perry, e-victim advocate and cyber-stalking expert, suggested that Network for Surviving Stalking (NSS) should embark on a project focused on the technology aspects of cyberstalking, the outcome of which could be a set of guidelines for victims to help them understand and learn to deal with the day to day risks presented by digital technology. Setting up the project, getting funding and managing the complex range of issues seemed in itself an enormous challenge: the expanding array of potential risks to victims could prove overwhelming; nothing quite like this had been done before and there might be resistance or apathy from the industry. Jennifer's vision, confidence and practical optimism got us started however and this was soon backed, quite inspirationally, by the Nominet Trust in the form of a grant, ongoing interest and support. Very quickly, during the consultation phase of the project, considerable enthusiasm was demonstrated by relevant experts with invaluable advice. Colleagues in NSS have played an indispensable role throughout, providing support to Jennifer and networking with interested parties. Then, towards the end of the project, the creation of an exciting partnership with Women's Aid, which has helped to ensure that we have an effective launch of the guidelines, as well as the very real possibility of working together on some of the challenges which have arisen as a result of the original project. So it gives me deep satisfaction to commend this work to all those who will read the guidance and practical advice. I hope you will find what you need and be safer as a result.

Peter Patrick
Chair, Network for Surviving Stalking



Women's Aid, as the national charity working to end violence against women and children, is delighted to be partnering with Network for Surviving Stalking to publish and promote this important resource for victims of stalking and anyone providing help or support to stalking victims. As research and practice experience has shown, stalking is a frequent aspect of domestic and sexual violence, and stalking disproportionately affects women victims who are most likely to be at risk of physical assault and fatal harm. In more recent years, with the advent of mobile and other digital technologies, stalking victims have been subject to abuse by increasingly hi-tech means. For Women's Aid, the continuing development of digital technology itself is problematic: on the one hand there are more opportunities for abusers to use technology to their advantage to continue to try to control and terrorise; on the other there are more opportunities for women trapped in abusive relationships to seek and receive support online. Understanding the risks to personal safety inherent in all aspects of digital technology is therefore no longer an option, it is a necessity. In publishing the first UK in-depth guidance of its kind, Women's Aid hopes that this will help enhance the safety of all victims of abuse. Our aim is to continue to update this information online as technology develops and changes, to enable continued protection and the prevention of future harm.

Nicola Harwin CBE
Chief Executive, Women's Aid

Preface

Stalking affects millions of people in the UK

Stalking is often perceived as only a crime against women. It is true that women are more likely to be victims of stalking and they are also more likely to be physically assaulted or murdered by their stalkers.

According to the Home Office, 9.3% of men and 18.7% of women have been victims of stalking since the age of 16 (UK Home Office, January 2011).

Offender characteristics

- 39% partners or ex-partners
- 36% known people (date, friend, acquaintance or colleague)
- 33% strangers
- 4% family members

(UK Home Office, January 2011)

In a survey on cyberstalking carried out by the University of Bedfordshire (Maple, Short and Brown, 2011) 35% of the victims who responded were men. Where women are more concerned about injury, men are significantly more concerned about damage to reputation and financial loss. Men are more likely to be harassed using instant messaging (IM) and work e-mail. Men were also more likely to experience harassment by work colleagues.

In the same study, women were more fearful than men of being physically assaulted. Women were most likely to harassed by an ex-boyfriend (21.2%) or ex-partner (10.4%). Women reported being harassed more via mobile phone/texts. Both sexes report significant harassment via social networks. The University of Bedford study demonstrates that perpetrators will use multiple forms of technology to torment their victims.

Survivors of domestic violence

Stalking by ex-partners accounts for the largest group of victims, with the majority of these victims being women. 80% of women in this group were previously physically assaulted while in the relationship. In approximately 50% of the cases the stalking behaviour started while they were in the relationship (Mullen, Pathe and Purcell, 2009).

Survivors of domestic violence are at higher risk of physical harm. The Metropolitan Police found that 40% of domestic violence murders were also victims of stalking (ACPO Homicide Working Group, 2003).

This group of stalking victims needs to take extra precautions, not only because of the risk, but also because the stalker often has much more information about, and insight into, the victim. S/he also has greater opportunity to access the victim, for example s/he might still live with her or they may be separated but share friends, financial assets, or caring responsibilities.

Digitally assisted stalking versus cyberstalking

Today, most stalking now includes a 'cyber' or technology aspect. Stalkers who stalk offline will usually assist their activities with some form of technology as a tool, e.g. mobile phones, social networks, computers or geolocation tracking. This can be characterised as 'digitally assisted stalking', as opposed to cyberstalking where the perpetrator uses technology but doesn't stalk the person in the offline world.

However, pure cyberstalking still inflicts the same amount of psychological damage, with many victims suffering from Post Traumatic Stress Disorder (PTSD) (Maple, Short and Brown, 2011).

Some of the technology which is available to stalkers is very inexpensive; other items cost a few hundred pounds. They are easy to find online with a quick search such as "spy on a computer" "locate my phone" or "track my wife". Many of these tools are quick and easy to use, others require more effort. Stalkers by their nature are persistent and will often find the time, money and skills to use technology against their victims.

Introduction

We all use a variety of different technology such as mobile phones, e-mail, online shopping and social networks. However, using this technology can put stalking victims at risk. It is important that support professionals and victims understand how technology works, why it puts them at risk and what steps they can take to reduce those risks. These guidelines review the most commonly used technologies and their risks. There is a section on spoof text (SMS) and global positioning satellite (GPS) car tracking devices, but the key risks are set out below.

Digital footprints

When we use technology it leaves 'digital footprints' which can include personal and financial information, our internet usage, our location, details of friends and much more. The difficulty for stalking victims is that their abuser looks for, and thrives on, any information he can obtain about his victim. Stalkers by definition are obsessive. They use social networks, work websites, forums and directories to gather information on victims – such as names of friends, contact details, work details, photos, or whether they are dating someone new. The stalker won't only be looking at the victim's online information, they will also be examining friends, work colleagues, and anyone connected with the victim.

If the stalker knows the victim well enough to know the victim's password, or guess their answers to security questions, he can access private information such as e-mail accounts, online calendars, and financial details of credit card and bank accounts.

All these techniques provide stalkers with the information they need to harass, intimidate and humiliate their victims.

Social engineering

While confidence tricks are normally employed for financial gain, similar techniques known as 'social engineering' are used to trick the victim or others into divulging information, harassing or humiliating the victim. Stalkers will use their knowledge about the victim in order to gain confidences and credibility so that they can manipulate others into helping them.

While tricking people into revealing passwords and other security information is the classic form of social engineering, other forms include posting provocative comments online, encouraging others to send abuse to the victim, having unwanted gifts sent to the victim, pretending to be the victim, changing their mobile phone contract, contacting friends and spreading lies in order to disrupt their relationship, or causing problems for the victim at work.

Mobiles

According to the National Stalking Helpline, the police, and domestic violence professionals, the technology used most to harass victims is the mobile phone. Mobiles are extremely powerful and the technology is advancing at speed. The difficulty is that new features and applications are being developed without properly considering the privacy or security implications. New technology is sold to consumers based on the benefits it offers – but they are given no explanation of the risks, especially for potential stalking victims.

People don't want to live without their mobiles. They contain our photos, music and texts, they allow us to surf the net, post to social networks and offer thousands of apps. The mobile phone is seen not just as a tool, but as an extension of ourselves. Two studies in Finland found that mobile phones can form an important part of the identity and image of adolescents (Boberg, 2008) (Ling, January 2001).

Because mobiles have become so integrated into many victims' lives, and are often a very expensive investment, it isn't sufficient to advise victims simply to get rid of their sophisticated phones. Victims have to be educated and helped to secure their phones and make informed decisions about which apps they could use and which apps they shouldn't.

Geolocation

This is the ability to identify the location of a device such as a mobile phone, camera, computer or tablet. The location information can be accessed by an application, or stored within a picture. Google Maps uses location information to give you driving or walking directions, or where to find shops and restaurants, but in order to do that it has to know where you are.

However, a stalker could use the same location information to track a victim, which could put them at risk of harassment or physical harm.

There are different ways a stalker could obtain the location information. If the stalker has had access to a victim's mobile phone they could download tracking software on it. Or a victim could be using an application such as Facebook Places, which tells anyone who can view their profile where the victim has most recently 'checked in' from their mobile. Victims can also share information by accident if they do not turn off the option to add geolocation information to photos.

Computer spyware

Computer spyware is another key threat for all victims of stalking. Often sold as legitimate employee or child monitoring software, it allows stalkers to control the victim's computer, read e-mails, see passwords, capture chat messages, and access stored information.

The perpetrator just has to trick the victim into opening an e-mail. The software is then installed by stealth on to the PC. It is often undetected by their anti-virus software. Victims will say, "I

don't know how he is finding out all this information", "my passwords keep changing", "He seems to know everything that is happening".

Social networks

Social networks went mainstream with the arrival of Facebook. No longer did social networks focus on chatting with people who shared an interest. Facebook managed to create a gathering place for friends and family to exchange photos, share jokes, update people on their latest news. It was easy to use and more importantly they managed to get people you knew to join.

Victims find social networks can provide the support and comfort they need to cope with their difficult situation. If the victim leaves the social network, they not only lose their support but they also find that they become increasingly out of touch with friends and left behind in their social circles.

On the other hand, the reason why it is so hard to protect victims on social networks is because information leaks from the profiles of friends and family. So, even if you can get the victims to tie down their privacy setting – it won't be effective unless all their contacts also do the same. Unfortunately, there isn't a one click option from Facebook for vulnerable people to lock down their privacy settings appropriately.

Advice and guidance

To make it easier to read, the advice in these guidelines is written as if the stalker is male and the victim is female, but it applies just the same to both male and female victims being stalked by perpetrators of either sex. In-depth advice is provided by a series of fact sheets including 'What tools are available for victims', 'Gathering evidence' and 'Warning signs of a cyberstalker'. In addition to the advice that is relevant to every victim or potential victim, specific additional sections give guidance for domestic violence survivors and those being stalked at their workplace.

Glossary

When using this guidance please refer to the glossary at the end of the guidance should you come across any unfamiliar terms.

Digital footprint

When using mobiles, websites, social networks, forums, e-mails and other online services you leave behind a digital footprint, and information other people leave online about you is called your digital footprint or shadow. Everything you do online leaves a trace. Your internet protocol (IP) address, website logs and cookies can be used to track what you've been doing online.

However, when it comes to stalkers, of most concern are the online communications, photos and information that are available publicly via social networks, blogs, work websites, comments posted in online forums and other online publications.

Our public footprints, the information that we freely publish, can give a stalker information that will feed their obsession or be used to help them intimidate, humiliate and harass. Our online information can be used to establish a pattern of where we go, who we know, how we are feeling – all giving the perpetrator insight into their victim. There may be contact information that could be leveraged to commit identity theft. There may also be specific information that the stalker could use to find their victim's location, such as the Facebook application that 'checks you in', telling everyone who can see your profile where you are/or have been at that particular time.

'Private' footprints also create a risk. This is the digital information that is available online that is considered 'private', usually being accessed by a password. It will include information stored 'in the cloud', such as e-mail accounts, calendaring applications, online bank or store accounts (Garfinkel and Cox, Feb 2009).

It is important that stalking victims try to minimise the amount of information that the stalker can access. However, many victims will have had a digital life, and footprint, before they became a victim of stalking. Trying to remove a digital footprint can prove difficult because although some information can be deleted there will be other information that can't be erased. Then the only option is to try to reduce the risks by knowing what is out there and making necessary changes so that information is obsolete.

Risks

- **Physical danger.** Obtaining location of a victim and committing physical assault or murder.
- **Contact information.** The perpetrator is able to find home, work, family and friends contact details.
- **Identity theft.** The abuser finding enough personal information to perpetrate identity theft.
- **Data gathering.** Stalkers are obsessive, they will look for every opportunity to gather information to use for social engineering to harm victims.
- **Account takeovers.** Our digital footprint reveals a lot about us. Most people use a password that is closely associated with them e.g. a pets name, home town, favourite football club etc.

Recommendations

Assess what online information exists about you

Perform online searches on your name, e-mail address, and phone numbers to see what information exists online. Remove as much content as possible either by deleting accounts or changing privacy settings.

Immediately change your e-mail and passwords for key online accounts

One of the first things perpetrators will try to do is 'hack' or access your online accounts. Immediately go to a safe computer, such as a friend's, and change your password (see Appendix D: Password security tips, pg. 48) for your main e-mail and other online accounts. Set up a new e-mail account (see Appendix E: E-mail – creating new accounts, pg. 51).

Online accounts that have profiles or online presences

Delete existing online accounts especially if they contain large amounts of information or photos. Decide if you want to set up new ones. If you set up new online accounts, limit those who you communicate with online to your most trusted friends. Think about what information you share with others – could it put you at risk? (see Appendix F: Share cautiously, pg. 53)

Review all the privacy and security settings

Check all your accounts but especially social network accounts to make sure that you have the highest possible security and privacy they offer. Privacy settings frequently change so regularly check them e.g. once a month.

Avoid public forums

Don't participate in public forums where the perpetrator can easily see your postings. Private forums can also pose a risk. An abuser can use false name to access a private forum. If you are participating in any forum be careful not share sensitive information.

Social engineering

Social engineering is when a perpetrator manipulates someone to divulge confidential information. A stalker will gather information about their victim that enables them to trick others into giving him more information or defraud them. Stalkers can be very manipulative and persistent and they will often use social engineering to gather information about the victim, e.g. finding where they are, their new phone number, e-mail, where they work, or if they are seeing someone.

Stalkers will use any information available to manipulate others. That is why social networks are so dangerous for stalking victims. Perpetrators will use a friends list and information posted within social networks to find and contact the victim's friend. He will e-mail or call, posing as another friend, saying they need to get in touch with the victim but they changed their e-mail address – and because he has information from things posted online he is able to be convincing and sound credible. Well-meaning friends will give out information such as mobile numbers or e-mail addresses without realising the threat.

Example: A friend posts on the victim's Facebook wall "hope your doctors appointment went ok" the stalker can use that information to contact a family member saying that he is from the GP surgery and needs to discuss some test results with the victim but has an old number. The family member instead of saying "I will have them call you", gives the imposter the victim's new phone number.

There are hundreds of ways a stalker will engineer a situation to get information, humiliate or abuse a victim. Technology helps them by making information available online that they can use against the victim.

Risks

- **Physical danger.** The biggest risk to stalking victims is the stalker obtaining the location of a victim and perpetrating a physical assault or murder.

Stalker uses eBay account to find ex-partner

A domestic violence survivor's ex-partner was monitoring her eBay account.

When she purchased an item, he waited a few days and contacted the seller claiming the item hadn't arrived. He asked the seller to verify the address. The seller inadvertently gave the perpetrator the victim's new address.

The perpetrator then found the victim; beating her so severely she was left blinded in her left eye.

Soliciting sex online

A stalker created a fake profile on adult websites. He went online pretending to be the victim and sent men photos of her.

He then solicited them for sex, arranged a time and sent the men the victim's address.

The victim was not at home, but her 15 year old daughter was home alone. Fortunately for the girl, the men left without incident.

- **Data gathering.** Stalkers are obsessive, they will look for every opportunity to gather information about their victim. They use this information to manipulate a situation or others that will help them abuse, intimidate or torment their victims.
- **Access to the victim.** The perpetrator uses social engineering techniques to get a new phone number or e-mail address, or trick the victim or their friends into adding them on a social network. Having established contact, they can begin the cycle of abuse again.
- **Installing spyware.** Spyware is a piece of software that can monitor the victim's computer. In order to install spyware the perpetrator has to trick the victim into opening what looks like an innocent file such as a photo or file. (see Computer monitoring/spyware, pg. 24)
- **Access accounts.** Victims often use e-mail addresses, passwords, PINs and security questions that the stalker either knows or can guess by picking up clues online. Once they have access to an account the perpetrator can fraudulently buy goods, transfer money, change passwords, or use a friends list to contact friends and family to harass them.
- **Manipulates others to help him.** The online information allows perpetrators to contact friends/family/colleagues.
- **Identity theft.** The perpetrator is able to pose as an imposter either online or offline either for financial gain or to humiliate the victim.

Recommendations

Clean your computer

Spyware/monitoring software is easy to find, cheap and can be installed remotely. All victims should assume they have spyware on their computer and act accordingly. So, the first thing to do is get the software removed by using an anti-spyware product (see Appendix J: Security tools for victims, pg. 61).

Change all passwords and pin

One of the key recommendations to all victims is to change all passwords and PINs. It is a key vulnerability for victims and is the first thing victims must do. Use a friend's computer, or one at a library, until you have made sure that your own has been cleaned up. Once you are confident your computer is spyware free, you should change ALL passwords and security questions. Choose ones that your stalker won't know and cannot guess (see Appendix D: Password security tips, pg. 48).

Limit what you share

For perpetrators to use social engineering techniques they need enough information to manipulate others to divulge information or do something on their behalf. Limiting what you say online will reduce the amount of information/data available to the perpetrator (see Appendix F: Share cautiously, pg. 53)

Educate friends, family and work colleagues

It is very important that all those that you discuss your life with or have access to you understand the risks a stalker poses. You must explain to them how stalkers use social networks to gather information and ask them to use high security settings on social networks. Instruct them never to give out e-mail, phone or address information, instead they should always ask who is calling and take a number so you can return the call.

Gather evidence

You need to keep a log of all abuse that happens online including on any social networks. Capture screen shots of offending posts, note if they try to make contact using new profiles or if they contact friends and family (see Appendix C: Gathering evidence, pg. 46).

Mobile

The biggest advancement of consumer technology in recent years has occurred in mobile phones. The mobile phone has become an indispensable part of many people's lives. According to a recent report (OFCOM, April 2011), 91% of all adults use a mobile phone. Smartphones are the highest growth area in the mobile market. The market research firm IDC forecasts that in 2011 smartphone sales will reach 472million worldwide.

A smartphone is a phone that has an operating system that offers more features. They enable people not only to talk and text but e-mail, use social media, surf the net, play games and pay bills. They can hold your music, video and photos. Of course they also hold important data about us such as our contact information, diary, passwords, photos etc.

It is all the new exciting features and apps available on smartphones that can increase the risk for domestic violence survivors and stalking victims. Smartphones not only contain sensitive information and apps that leak data about us, they can also lead people to our exact location.

Growth of smartphones and mobile internet use

Over a quarter of adults (27%) and almost half of teenagers (47%) now own a smartphone according to OFCOM's latest Communications Market Report (OFCOM, August 2011). Most (59%) have acquired their smartphone, which includes devices such as iPhones, BlackBerrys and Android phones, over the past year.

A nation addicted to their smartphones

According to OFCOM, people have become addicted to their smartphones: "Users make significantly more calls and send more texts than regular mobile users (81 per cent of smartphone users make calls every day compared with 53 per cent of 'regular' users). Teenagers especially are ditching more traditional activities in favour of their smartphone, with 23 per cent claiming to watch less TV and 15 per cent admitting they read fewer books. And when asked about the use of these devices, 37 per cent of adults and 60 per cent of teens admit they are 'highly addicted'." (OFCOM, August 2011)

Mobiles form part of teens' identity

"The mobile telephone is not simply a functional device used for communication but rather is an element in the very presentation of self."

(Ling, January 2001)

Realistic advice

Mobiles provide contact, support, security, access to information – in other words they are now indispensable. They are also costly. So, although we could have advised that victims put away their £300 phone and go back to an old-fashioned voice-only mobile, this just isn't realistic and would not be followed. Instead, we provide advice as to what the risks are with smartphones and how they can be used more safely.

Mobile spyware threat

Spyware is software designed to gather information about your phone usage and make that information available via online or text. Unlike computer spyware, the perpetrator has to gain physical access to the phone in order to install the software. The perpetrator will go online beforehand and purchase the spyware and get a code. Then when he has access to the mobile he uses it to access the spyware company's website, enters the code and the software is downloaded. This process takes less than five minutes.

Here is what one mobile spyware company advertises:

The following are features available from Flexispy.com products. Their products range from \$149-\$349.

- **Remote listening.** Make a spy call to the target phone and listen in to the phones surroundings (it does not allow you to listen to the phone conversation in progress).
- **Control phone By SMS.** Send secret SMS to the target phone to control all functions. No further need to physically access the phone.
- **SMS and e-mail logging.** All SMS and e-mail contents are sent to your web account.
- **Call history logging.** The time, duration and number of all voice calls are sent to your web account. If the phone number is in the phone's address book, then the name will be provided as well.
- **Call interception.** The ability to listen in to an active phone call on the target device. You specify the numbers you are interested in and when any calls to or from these numbers occur on the target a secret SMS will be sent to your mobile.
- **GPS tracking.** For devices that have GPS hardware, you can see the co-ordinates of the device in your reports when you log into your web account.
- **Shield.** Hide all activity from specified contact in a hidden database (MMS, SMS, phone logs).
- **Blacklist.** Reject calls from blacklist.
- **Whitelist.** Accepts calls from whitelist only. All other calls are rejected.
- **View report.** Log in to your account to view all the location SMS, e-mail and phone activity in an easy to use format.
- **SIM change notification.** When the SIM card is changed, a text message is sent to a number you specify. This lets you know the new phone number, and you can continue to control the device because you know its new number.

Warning signs of spyware on your mobile

Spyware is designed to hide, but it does leave some clues, so here's what to look out for:

- **Has someone borrowed your phone or had access to it?** In order to install spyware on a mobile the perpetrator has to have physical access to the phone. They have to be able to access the internet and download the software on to your phone.

- **Check your mobile phone bill.** Spyware will send out texts and upload data. So, keep track of how many texts you send over 48 hours and see if it matches your bill. Do the same for your data usage (apps are available that can check your data usage). If either of these are higher than you expected one of the explanations could be spyware.
- **Your battery isn't lasting as long.** Spyware tends to drain your battery. It might be checking the phone's position, sending texts or making secret calls, and this can shorten your battery life.
- **Your mobile turns on unexpectedly.** If your mobile 'lights up' and doesn't ring that is a warning sign. Some spyware's remote listening features can't prevent the phone from showing the incoming call.

Risks

- **Harassment.** Because we carry our mobiles with us at all times, perpetrators will call, text and leave voice-mails. It isn't unusual for a stalker to make contact frequently during a day – every day.
- **Feeding obsessive behaviour.** Using a mobile for surveillance provides the stalker a feeling of control and gives her/him gratification.
- **Physical danger.** If the victim's mobile either has spyware installed or a geolocation app (see Geolocation, pg. 20) that the abuser can access, they can learn where the victim is or see a pattern of the victim's habits.
- **Invasion of privacy.** Spyware can turn on the camera or microphone, and send the results to the stalker.

Recommendations

If you are leaving an abuser

You should assume that your abuser has installed software or an app that can track you. Turn off your phone and **REMOVE** the battery. You can pick up an inexpensive phone at a supermarket for about £10. Once you are safe then you should clean your phone.

Clean your phone

If an abuser has had access to your phone, he may have downloaded software or an app that can track your movements, leak information or spy on you by turning on your phones voice and camera features. If you suspect your phone has been tampered with you should back-up your photos, music, address book and any apps you want to keep. Then you should do a factory reset. This will delete any unwanted software.

Smartphone users are more likely than those with any type of mobile to:

- visit websites (53% vs. 19%)
- e-mail (50% vs. 16%)
- take photos (63% vs. 34%)
- use social networks (39% vs. 15%)
- listen to music (45% vs. 22%)

(OFCOM, April 2011)

Secure your phone

Set the phone so that if it isn't use for more than a minute you have to put in a PIN to use it. Your stalker might have access at your workplace or be a partner who started stalking behaviour before you broke off the relationship.

Make sure that your phone is set to hide your caller ID.

Anti-virus/spyware software

In order to put spyware on a mobile the perpetrator has to have access to the phone. If you don't think this has been possible then you probably don't have spyware. However, since today's smartphones are starting to come under attack from online malware it is still a good idea to use antivirus/spyware software (see Appendix J: Security tools for victims, pg. 61).

Use whitelist call blockers

There are mobile phone applications that will block calls. You want to choose an application that offers a 'whitelist' feature. This means that it will only accept calls from those in your contact list. A 'blacklist' feature blocks specific numbers. However, perpetrators will simply call the mobile from a new number to get around a 'blacklist'.

If you are using a whitelist feature then remember to add contacts such as the doctor's practice, school, solicitor and your police contact details. You may also want to consider getting an inexpensive mobile for the limited people who may need to get in contact with you but who may be calling from an office that sends out different phone numbers. Or ask that person to use a dedicated phone number when they contact you.

Whitelist applications offer different options such as picking-up the call and immediately hanging up or sending it to voicemail. Both of these options could help you gather evidence. Your call logs will show calls coming in and you can replay and record the voicemails. Many mobile security products offer a whitelist feature (see Appendix J: Security tools for victims, pg. 61).

Choice of phone

Try to avoid having a smartphone with a camera that faces the user. Stalkers can use spyware to send a message to the phone, and then take a photo of you when you touch the screen.

Gather evidence

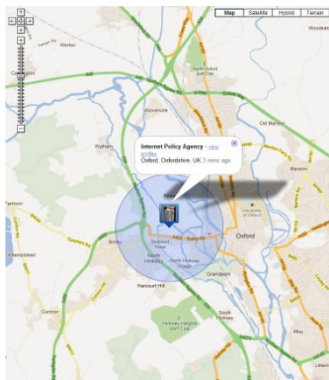
Save all texts but also take pictures of any threatening messages on your phone. That way if anything happens to your phone you still have evidence of the text. Make a recording of ALL voicemails left on your phone. Mobile operators limit how long (on average one week) they will keep the voice mail on the system. Once that time is expired they delete the voicemail and that evidence is gone (see Appendix C: Gathering evidence, pg. 46).

Geolocation

Mobile electronic devices are increasingly aware of their location, which can be used to enhance the user's experience, or sent to others either deliberately or accidentally. Originally restricted to items such as satnavs, the inclusion of GPS (Global Positioning System) and other technology allows modern phones to incorporate advanced features such as location-stamping of photographs and adding location-awareness to desktop applications such as weather forecasts and travel information.

How a coarse location is calculated

A mobile phone (or tablet with 3G data) is constantly in contact with nearby phone masts, each of which has been accurately mapped by the phone companies. An approximate location of the device can be determined from the signal strength (number of bars), which is an indication of the distance from nearby masts. By combining the results from two or three masts, in urban areas it is possible to get a location accurate to better than half a kilometre. In rural areas the accuracy may be less.



The position obtained in this way is also known as the 'network-based' location, and as well as being calculated by the handset with the help of online databases which know where the masts are, the mobile phone network operator can make the same calculations and therefore track the position of the device independently. Some mobile networks sell their own location services, for example to employers to track the whereabouts of their staff. It is not possible to track a phone that is switched off, but some spyware may make a phone pretend to be switched off – removing the battery is a sure way to disable the phone.

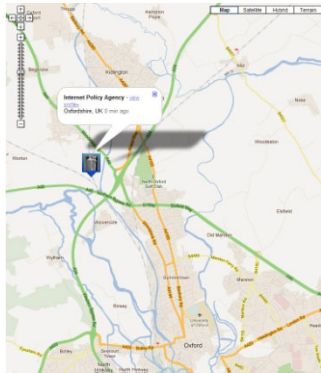
Alternatively many devices, including laptops and phones, include wi-fi connectivity, and will be scanning for nearby wi-fi points, both public and private. The identity of those wi-fi points can be determined even without the user connecting to them. By consulting a (large) database of the locations of wi-fi points, the device can locate itself within a few hundred metres, and possibly much closer.

There are several such wi-fi databases, built by vendors either by driving along the streets and logging the wi-fi points as they pass, or indirectly by collecting the information from other users whose handsets have been logging their location and nearby wi-fi points, and submitting the data periodically. As with network-based location, the calculations are done automatically by the application, and the user simply sees the result, often as a circle drawn on a map.

How a fine location is calculated

GPS receivers work by receiving signals from four or more of a total of thirty satellites, nine of which are always visible in the sky at any place on Earth. The signals are weak and therefore the technology generally only works outdoors or next to a window. An accuracy of about 20

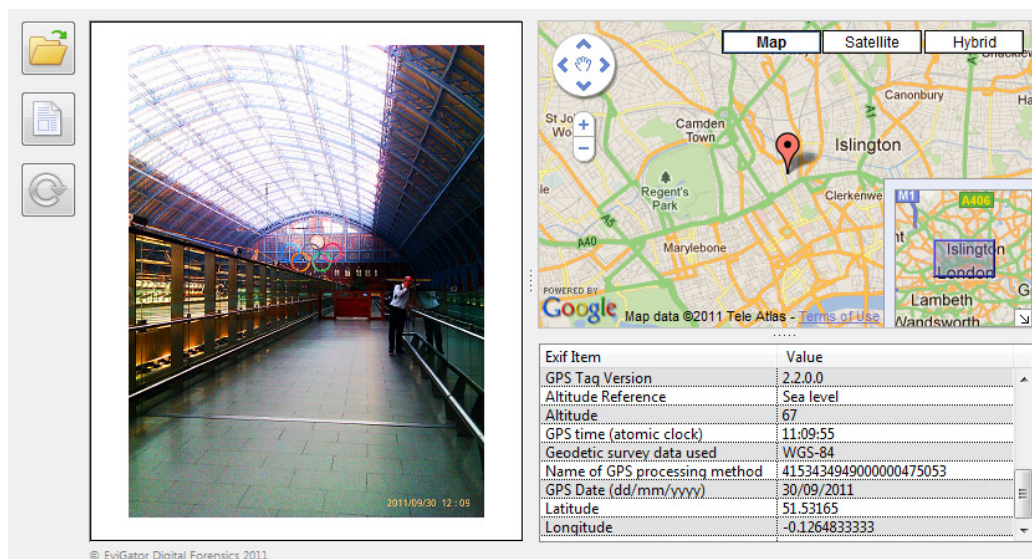
metres can be achieved by comparing the transmission time (and therefore the distance) between the known position of the satellites and the receiver.



Nothing is sent from the GPS receiver to the satellites, and therefore the position is known only to the receiving device. GPS receivers can use a lot of battery power, and so many users will switch the function off. But be aware that applications (both friendly and malicious) can switch it back on again, possibly for just a short time until a new location has been determined. GPS receivers can calculate their position much faster if they start by knowing roughly where they are, and a system called Assisted GPS (AGPS) primes them with the network-based location.

Geotagging of photos

Most phones have a camera, and smartphones in particular can optionally add geotags to a photo which give the location. Most common is GPS tagging, which allows the automatic positioning of photos when uploaded to mapping sites (e.g. Google Panoramio). Sometimes other tags, such as the identity of a nearby phone mast, will be added. Some social networks and picture sharing sites strip off the geotags from uploaded images.



Location from IP address

Using an IP address to locate from which house an internet connection is made can only be done with the co-operation of the victim's internet service provider (ISP), which should be limited to law enforcement professionals and a handful of public authorities using powers within the Regulation of Investigatory Powers Act (RIPA).

Websites which purport to locate a user based on their IP address will normally return the address of the ISP, or possibly one of their regional offices, so is seldom more accurate than

within 20 miles or so. These websites do not have access to the information regarding individual users, nor can they calculate the location from any tests they might conduct. For users with mobile internet (3G) connections, the IP address bears almost no relation to their location at all, although it's possible that wi-fi users could be traced to the IP address of a wi-fi hotspot.

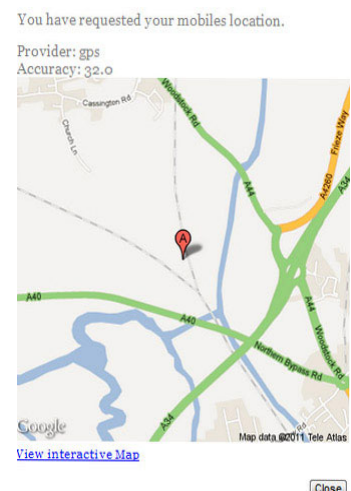
Risks

- **Physical danger.** Allows the abuser to know where the victim is or see a pattern of the victim's habits. Leakage of the 'fine location' can reveal the building a victim is in, and the 'coarse location' which village or suburb. In rural areas, despite being less accurate, it could also reveal where the victim is living. Access to a satnav or satnav application can reveal a list of 'recently visited' places.
- **Burglary or tampering with possessions.** Knowing that the victim is at work could result in a stalker targeting their home or vehicle.
- **Hunter hunted.** Applications such as 'find my lost phone/laptop/child' can be used against the victim if the stalker manages to gain access to the necessary accounts and passwords.
- **Undocumented logging.** Some phones collect location data which is then periodically collated centrally. Traces of these logs may be accessible if a stalker has the opportunity to examine a phone.
- **Unintended phone behaviour.** Some phones have design faults such that they send location data even when the user has switched the feature off.
- **Mission creep.** Location services are in their infancy, and it's possible that data being collected will be used in ways which were not anticipated. Many application developers request too many privileges from the user when initially installed, which may result in future enhancements to their product becoming a risk without them having to re-confirm the permissions.

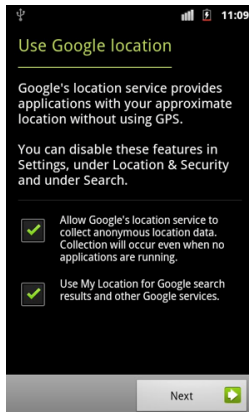
Recommendations

Use GPS facility with great care

Devices with GPS location built in often have a special symbol (which varies by phone) on the screen to show that they are active, and it will normally change to a different symbol when it has acquired a 'fix'. Applications which wish to use GPS location should ask permission from the user, but this setting is remembered by the device and can be easily overlooked. Make sure you understand how to tell whether the GPS is switched on or active (see Appendix I: Disabling mobile pictures' geotags, pg. 58).



Restrict location data



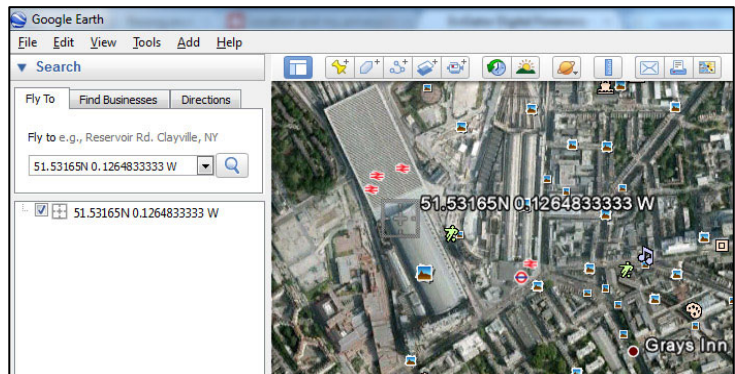
Don't give applications permission to access your location data unless you fully understand the implications. Turn off the GPS facility on devices unless it's absolutely essential. Knowing the coarse location is sufficient for many applications and perpetrators.

Some smartphones will only geotag a photo if a fine (GPS) location is available, but others will default to a coarse (network) location instead.

Make sure photos don't contain metadata

When you take a picture on your mobile it adds metadata, hidden pieces of information attached to a photograph which can reveal the location of where the photo was taken (for example, when you upload the picture to a website).

Understand how to turn off geotagging on your camera phone. You will probably have to switch off the geotagging settings in the camera application, as well as making sure that the phone's location services are set appropriately (see Appendix I: Disabling mobile pictures' geotags, pg. 58).



Use a utility program to examine photographs to see if they have any tags, for example FileTagSleuth (www.ulfwood.com) or TAGView (www.evigator.com/free-apps/).

You can also use a utility to strip them off, such as Exif Tag Remover (www.rlvision.com/). If required, Google Earth can very easily translate latitude and longitude geotags into a position on a map.

Computer monitoring/spyware

As with mobiles, there is computer spyware/monitoring software available to buy online. Unlike mobiles you don't have to have physical access to the computer to install it. This software is easy to find via an internet search. It's cheap, easy to use and very powerful.

This software is sold legally as a monitoring product for children and employees. However, because it will have features like remote install and because it is hidden from user view when it is running, it is ideal for stalkers to use.

So even if you don't think your computer has been compromised, **your safest bet is to assume it has been**, and that everything you do or say online, including your passwords, calendar, e-mail, contacts, is being monitored until you've cleaned up your machine.

Spyware available online

spytech-web	\$69.99
Webwatchernow	\$97.00
Sniperspy	\$79.97
Spywaredirect	\$82.99
i-spyware	\$89.95
remote-spyware	\$89.95
Simplekeylogger	\$39.95
Smartkeylogger	\$59.95

How do perpetrators put spyware on a computer?

These spyware products help perpetrators disguise their software so they can trick victims into putting it on their computer. The perpetrator sends a victim an e-mail that has a file attached; it could be a picture, PDF or other document. When the victim opens the file the spyware is downloaded in the background without the victim knowing.

What does spyware do?

The most common features include:

- showing all key strokes;
- capturing all IM chat conversation;
- showing all websites visited;
- monitoring what is written online and in social networks;
- providing the ability to read your e-mail;
- showing usernames and passwords;
- capturing screenshots of what you are doing on your computer;
- turning off the computer, moving the mouse, launching applications;
- enabling stalkers to up load or delete files.

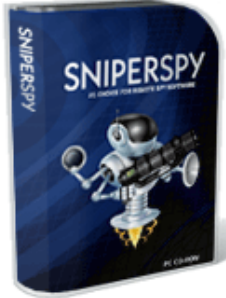
What is SniperSpy remote monitoring software?

No physical access to your remote PC is needed to install the monitoring software. Once installed you can view the screen LIVE and browse the file system from anywhere anytime. You can also view chats, websites, keystrokes in any language and more, with screenshots.

This software remotely installs to your computer through email. Unlike the other remote monitoring titles on the market, SniperSpy is fully and completely compatible with any firewall including Windows XP, Windows Vista and add-on firewalls.

The program then records user activities and sends the data to your online account. You login to your account SECURELY to view logs using your own password-protected login. You can access the LIVE control panel within your secure online account.

[VIEW DEMO ▶](#)

The image shows a software box for 'SNIPERSPY'. The box is blue and black with a graphic of a sniper rifle. The text 'SNIPERSPY' is prominently displayed at the top.

Risks

- The software monitors all communications including e-mail, chats and social networking.
- It allows the perpetrator to find out your username and passwords so they can:
 - lock you out of your account;
 - access financial accounts and buy goods or transfer money;
 - go online and pretend to be you – posting offensive material, damaging your reputation and relationships.
- It gives the ability to access, alter, add or delete files on your computer.
- Software reports what websites you visit.
- It allows the blocking of websites so victims can't access support sites or social networking sites.

Recommendations

Use a safe computer

Until you can get your computer cleaned stop using it and disconnect it from the internet. Go to a 'safe computer' at a friend's house and set up a new e-mail account (see Appendix E: E-mail – creating new accounts, pg. 51), change your passwords (see Appendix D: Password security tips, pg. 48) on all your online accounts. When you change your online accounts also check the privacy settings to make sure they are set to the highest level of privacy. **Do not use your old computer.** Do not access your new e-mail accounts or log in to accounts with the new password from your computer until you are sure that computer is safe.

Buy spyware removal software

Anti-virus software doesn't detect or prevent monitoring/spyware from being put on your computer. You have to buy software designed to look specifically for spyware. There are a lot of fake anti-spyware products online. Buy a well known, trusted brand.

Get a new email account

Your stalker may know your email/username and passwords on your accounts. Get a new email account(s) and this will increase your security on all your accounts (see Appendix E: E-mail – creating new accounts, pg. 51).

Secure password

Once your computer is clean and secure, create new, strong passwords to log on to computer administrator accounts and be sure you are the only person with access. Set yourself up as a user and create a new password to log on to your computer using that account (see Appendix D: Password security tips, pg. 48).

Block e-mails

Whenever you receive an e-mail from a stalker or a suspicious e-mail address, immediately add it to a block list. Most e-mail programmes and online services have a feature that blocks e-mail. Go to the help pages and put in 'block e-mail'.

What not to do

- Do not open attachments. Perpetrators can spoof a return e-mail address to make it look like it is coming from a friend's e-mail account. If someone you know has sent you an attachment, call or e-mail to confirm it is really from them.
- Do not open pictures/cartoons attached to jokes – immediately delete them.
- If you have children or someone else in the house using your computer, tell them not to open any attachments without showing them to you first.

Trusted anti-spyware

www.2-spyware.com	Reviews
www.malwarebytes.org	£19.95
www.pctools.com (spyware doctor)	£29.99
www.superantispyware.com/	\$29.95
www.webroot.com (spysweeper)	\$39.99
Microsoft windows defender	Free
(http://windows.microsoft.com/en-US/windows7/products/features/windows-defender)	

Social networking

You can NEVER make social networks 'safe' for victims to use you can only make them 'safer'. Ideally, a victim would deactivate their account to reduce their risks. However, social networks do offer support and reduce isolation so many victims are reluctant to leave their account. They must be given advice to minimise the risk, including how to improve privacy settings. They must also learn to share cautiously (see Appendix F: Share cautiously, pg. 53).

To appreciate why social networks are so dangerous, you have to understand how they work. Social networks have an inherent conflict. Their commercial success depends upon encouraging users to exchange information with the widest network possible, which compromises the privacy and security of their users. Indeed you could argue that it is in their interest not to encourage good privacy practices.

Social networks encourage the use of new features and applications, exposing the users to even more data leaks. The language that they use sells the 'benefits' of their features – it doesn't explain to users what is happening, what information they are accessing, what is leaking and what risks it could pose.

It is a challenge for users to operate the numerous and constantly changing privacy and security settings available. It is often unclear what option the user should choose to improve their privacy. This leaves users, particularly vulnerable groups such as stalking victims, at much higher risk.

The dominant social network is Facebook, and this section of the report will focus specifically on Facebook. However, if you are using a different social network the same principals apply, check the settings. The default settings on Facebook expose users' information to the widest possible audience. The network continually changes features and privacy settings (often without notification to users) making an account with previously high privacy settings less secure.

Facebook attracts a broad range of users from pre-teens to pensioners. Stalking also affects all age ranges but the risk of being stalked decreases with age. The highest risk age group is 18-24 (US Department of Justice, 2009). Teens are also at risk of stalking but there is no data on this group because it is an unrecognised crime: "The legal system knows how to respond to adults who engage in stalking behaviours, but currently, the system not only does not know how to respond to juvenile stalkers, it has no idea that teens engage in this behaviour." (Thomas M Evans PHD, J Reid Meloy PHD, 2010)

Woman murdered after she changed her Facebook status

On 12th March 2009, mother of four Haley Jones, 26 was murdered by her ex-partner Brian Lewis, 31 shortly after she changed her status from 'married' to 'single'.

Risks

- **Physical danger.** If a victim posts where they are living or if they are going out somewhere on their Facebook wall, a stalker could use that information to find and physically attack them.
- **Contacting friends.** One of the most common things that stalkers do is contact the victim's friends. They use Facebook to get a list of the victim's friends. Then they will ask to become 'friends' with them on Facebook and then access their phone number and e-mail address. They will contact them in order to gain more information about the victim or to sabotage those relationships to isolate the victim.
- **Data leak.** Stalkers will scour social networks for any information. They will read the victim's Facebook wall and look at their photos continuously. When victims make their account secure, the perpetrator will go to the victim's friends accounts (which are often less secure) to try to pick up any information or clues about what is happening in the victim's life. They will read the friends wall, look through the photos, scan their 'friends list' to see if the victim is listed or to find other mutual friends he can look up.
- **Feed obsession.** Stalkers are obsessed with their victim and they will spend hours a day on their fixation. They want to monitor their victim's emotional state, their relationships, developments in their lives, future plans, see new photos etc. They find any information about the victim gratifying. Social networks can provide an enormous amount of information in one place.
- **Trigger the perpetrator.** Change in status, new relationships being discussed online or photos can all trigger the stalker to react.
- **Social engineering.** Facts about the victim gathered on a social network can be used to trick others in giving out information (see Social engineering, pg. 13).

Recommendations

Block perpetrator and associates

You should block your abuser from your friends list on Facebook. Blocking them prevents them being able to view any information about you when they are logged into their Facebook account. They are not told you have blocked them. You should also block their friends and family as well as anyone who might view your Facebook information and tell the abuser what they saw or allow the abuser to use their account.

Limit friends

Limit Facebook friends to only those close friends and relatives that understand you are at risk. They need to help keep you safe by not sharing your information to anyone, not adding people they don't know and by using good privacy settings.

Use an anonymous name and fake photo

Create a user name that won't identify you. Make up a name and consider changing the gender. Change all the profile information, e.g. location. Find an online picture of an ordinary person to

use. The objective is to make the profile believable without providing any clues about the real user.


Password security

When setting up a new account, you need to use a strong password that your stalker can't guess. It needs to be something that no one would associate with you or be entirely random. (see Appendix D: Password security tips, pg. 48)

The most important thing you can do is to optimise your privacy settings and it is **very important** to have your friends also increase their security.

At the time of writing (October 2011), Facebook has five categories for privacy settings. The overall default setting should be 'friends'. Users should go through all categories and make sure each option is set to only 'friends', don't allow anyone to perform tagging, and disable search (see Appendix H: how to set Facebook's privacy settings to increase security, pg. 55).

Facebook privacy categories (October 2011):

- **How You Connect.** Control how you connect with people you know.
- **How Tags Work.** Control what happens when friends tag you or your content.
- **Apps and Websites.** Control what gets shared with apps, games and websites.
- **Limit the Audience for Past Posts.** Limit the audience for posts you shared with more than friends.
-  **Blocked People and Apps.** Manage the people and apps you've blocked.

Share cautiously

Think carefully about what you post online, for example, you should be careful about sharing personal contact information, your location, and talking about new relationships. Friends can also forward information about you to others or post something about you on their wall without realising it could put you at risk. Check what information friends are putting on their own wall about you and ask them to remove any comments that could put you at risk.

Delete any inappropriate content on your wall. If you need to vent anger and frustration it is better to do that in a more private forum such as calling or e-mailing a friend or family (see Appendix F: Share cautiously, pg. 53).

Photos

We all can have a laugh taking photos of ourselves or friends. Unfortunately, they can cause stalkers to react especially if they are sexually suggestive pictures, photos of new partners with you or your children and you may know of other things that will make him react. Although it is never your fault, it is always better to be ultra cautious. So, you should have your privacy settings so that friends can not tag you. If there are tagged photos of you then untag them.

Even photos without tags can give away a lot of information, for example a friend may take a picture of you at a pub that a stalker will recognise or where it shows the name. So ask friends to show you the pictures they've taken to make sure they are safe.

Don't let people take pictures on a mobile when you are around because they can be uploaded to the internet or distributed via e-mail. Those pictures could have a geotag and the stalker can tell the exact location where the photo was taken (see Appendix I: Disabling mobile pictures' geotags, pg. 58).

Educate friends, family and work colleagues

It is very important that the people you discuss your life with and others you associate with understand the risk a stalker poses. You must explain to them how stalkers use social networks to gather information and ask them to use high security settings on social networks. Instruct them never to give out email, phone or address information, instead they should always ask who is calling and take a number so you can return the call.

Account access/takeovers

Account access is when someone gains access (logs into) another person's account without permission.

An account takeover is when someone accesses another person's account, and then also changes the user name or password so the original account holder can no longer access their own account.

Account accesses and takeovers are one of the most common incidents experienced by stalking victims. If the perpetrator is an ex-partner they will often know the victim's e-mail/username and password so gaining access to online accounts can be easy. The username and password may even be stored on a PC previously used by the victim.

If they don't know the password, the perpetrator can often guess it, or use a 'lost password/username' feature to trigger an easy to guess security question (such as "what's your favourite colour?" or "where did you go on your honeymoon?"). If the perpetrator gains access to the victim's e-mail account, they can read e-mails containing password-reset information for other accounts belonging to the victim.

Stalkers commit identity theft

In 2009 stalking offenders committed identity theft against about 204,000 victims in the US. Over half of these victims had financial accounts opened or closed in their names or money taken from their accounts, and 3 in 10 of these victims had items charged to their credit cards without their consent.

Any identity theft	204,230	100%
Opened/closed accounts	110,850	54.3
Took money from accounts	105,130	51.5
Charged items to credit card	60,790	29.8

(US Department of Justice, 2009)

Even victims that haven't been in a relationship with their stalker are at risk. Guessing passwords isn't as difficult as most people think. Many people use easy-to-remember passwords that relate to their personal lives, such as the name of a pet, child, date of birth, city.

Stalkers will use information they already know, or information available via social networks, to try to guess passwords. Since the majority of internet sites allow you to try different passwords as often as you like, they are able to try over and over again until they figure it out.

The average internet user has 6.5 passwords for 25 different online accounts (Dinei Florêncio and Cormac Herley, 2007). That means if a stalker finds out an e-mail/password combination for one account it will probably work on many of the victim's other accounts.

Victims would significantly increase their security if they not only changed their password but also updated email addresses on all their accounts.

Stalkers can also use computer spyware to access information about the victim, including account log-in information.

Tell-tale signs that your account has been accessed:

- some (e.g. banking) have 'last accessed' dates;
- e-mails disappearing, or being marked/unmarked as read behind your back;
- e-mails that were sent to you disappearing before you saw them;
- registered details changing (for example, the e-mail address to which you send password recovery information);
- you receive an e-mail requesting you to confirm a new password request.

Risks of account access/takeovers

- The greatest risk is physical harm. The perpetrator can access an account that has the victim's current address and use that to find the victim and physically harm them.
- A 2009 US Department of Justice Study found that victims regularly suffered financial loss through abusers access to online bank accounts or store accounts¹.
- It can provide an opportunity to humiliate or defame their victim. If the perpetrator has access to accounts such as social networking or forums, they can post comments or pictures in the victim's name that are designed to humiliate or damage their reputation.
- They can damage or destroy relationships by accessing a victim's e-mail account to send family, friends, work colleagues or clients abusive messages, or messages telling them never to contact the victim.
- The perpetrator can use the victim's account to send themselves abusive messages in order to incriminate the victim.

Recommendations

Use a safe computer

You should go to a 'safe computer' such as a friend's or library computer and set up a completely new e-mail account. Don't access the new accounts on your old computer until it is known to be clean and it is protected by an anti-spyware product.

Create multiple e-mail accounts

It is important to create multiple e-mail accounts so if one gets compromised your other accounts are still usable.

¹ About 3 in 10 stalking victims accrued out-of-pocket costs for things such as attorney fees, damage to property, child care costs, moving expenses, or changing phone numbers, lost wages. US Department of Justice National Crime Victimization Survey – Stalking Victimization in the United States 2009.

Create an e-mail account for each of the following:

- close/trusted friends and family;
- colleagues, casual friends;
- financial accounts, e.g. banking, online stores etc;
- social networks, online registrations, newsletters etc.

Managing multiple accounts doesn't have to be complicated; Google, Yahoo! and many online providers now have multiple e-mail management features (see Appendix E: E-mail – creating new accounts, pg. 51).

Password security

When setting up a new account, you need to use a strong password that your stalker can't guess. It needs to be something that no one would associate with you. Don't use Firefox as your browser because if the abuser has access to the computer it is easy to see the stored passwords (see Appendix D: Password security tips, pg. 48).

GPS devices for a car

GPS technology has got smaller and cheaper. This has led to the development of GPS tracking devices the size of a match box that are attached to a car by a magnet. These are battery operated devices that can last up to a week. They work either by storing the location information which the perpetrator uploads to their computer, or the perpetrator can use a mobile to call the devices which will then text back the cars location. These devices cost £150 upwards and are easily found online.

Companies selling spy equipment such as GPS software, surveillance devices

www.onlinespyshop.co.uk
www.spyequipmentuk.co.uk
www.spycatcheronline.co.uk
www.eyetek.co.uk
www.msccspytek.com
www.spy-wireless.com
www.spytechnology.co.uk
www.lorraine.co.uk
www.spy-craft.co.uk

Risks

- **Physical risk.** This technology allows a stalker to know exactly where the victim's car is at a particular moment. This gives the stalker physical access to the victim even if they are trying to go into hiding.
- **Gather information.** The perpetrator can use this technology to establish patterns, determining who the victim visits and when.
- **Trigger the perpetrator.** If the perpetrator knows that the victim is going to the police, or someone he sees as a threat, it could create a response.

Recommendations

If you are leaving your abuser

If you live with the perpetrator and are trying to leave undetected, get a taxi/bus, or meet a friend in another road.

Park your car securely

If possible, park your car in a locked garage. Put motion detector security lights near your car. At the workplace park the car in view or near a security camera.

Ask neighbours to help

Ask your neighbours to help watch your car and your home. If you know your stalker, provide a picture so they can help keep watch.

Examine your car

GPS devices are usually secured to the car by magnets, are about the size of deck of cards, and are usually black. Use a torch and look for anything that may be a GPS device. Look around the wheel and bumpers. Remove it and report it to the police.

"GPS vehicle tracker: rapid deployment magnetic tracker. Credit card size. Request location by text message or call. Receive a full colour map direct to your mobile phone."



Spoof SMS

There are mobile apps and UK-based services that allow a perpetrator to send a text message and spoof the number (make it appear it is coming from a different number). The perpetrator can use any number. In order to circumvent mobile blocking software they could use a number the victim trusts, such as a relative. Alternatively they can send a text to their own phone using the victim's number in order to try and incriminate the victim. These services charge approximately sixty pence per text message.

Risks of spoof SMS

- The perpetrator can contact the victim via SMS and make it look like it comes from a friend.
- The stalker can send a text SMS to themselves, spoofing the victims mobile number to try and incriminate them or make it look like they are the victim.
- The perpetrator can send offensive text to friends, family, work colleagues in an attempt to cause relationship difficulties for the victim.

Recommendations

Educate the police

If you think you have been a victim of a spoof SMS and it is undermining your case with the police, you may need to educate the police about spoof SMS services. Tell them that you want them to check your mobile phone records to verify that you did not send that particular text.

Contact your mobile phone provider

You can ask your mobile phone provider to provide the police with your phone logs (list of incoming, outgoing calls/text). You will need to give the mobile phone company permission to release the information to the police, and provide a crime number and the police contact's name, address and phone number. The phone companies will send the information directly to the police.

Gather evidence

If the spoof SMS was sent to friend or employer ask if you can have a picture of the phone with the text on it as part of your evidence of harassment (see Appendix C: Gathering evidence, pg. 46).

Survivors of domestic and sexual violence

If you are planning on leaving

Don't use your home computer. Stalking behaviour often starts before a women leaves her home. All victims should assume that their computer is being monitored.

Do not use your computer or existing e-mail accounts to make plans or inform anyone that you are planning to leave. Use a safe computer (one that the perpetrator could not have installed software on or that they monitor) such as a friend's or a library computer.

Create a new e-mail account. Use a safe computer to set-up a brand new e-mail account. **Don't access the new e-mail account on your old computer** – remember the abuser may be monitoring it. Don't use password or security answers the abuser could guess (see Appendix D: Password security tips, pg. 48). Only use this e-mail account to contact those helping you to make plans.

Don't use your smartphone. When you leave, disable your smartphone so you can't be traced. Turn off your smartphone and remove the battery. Buy a cheap mobile phone. You can get them for £10 at a supermarket.

Check your car. If you plan on leaving in your car, check for a GPS tracking device (see GPS devices for a car, pg. 34). Consider using a taxi/bus or meet a friend in the next road. If you continue to use your car the abuser may try to find the car and you.

Once safe

Change passwords

As soon as possible, use a safe computer to change the password on your existing e-mail account(s). At the same time, change any secondary contact e-mail address to your new account(s). Remember to change your social network accounts, online banking, eBay, PayPal, online stores etc. You should call your mobile phone company and change the security PIN/passwords (see Appendix D: Password security tips, pg. 48).

E-mail accounts

It is better to use multiple e-mail accounts. It means if the perpetrator gets hold of one of them you have an indication of where there is a security issue. It also means if he gets hold of one e-mail account the others are still safe to use. If you use a service like Google mail you can manage them all easily. Create separate e-mails accounts for:

- most trusted friends and family;
- social networking – other friends;
- online registrations;
- financial account.

(see Appendix E: E-mail – creating new accounts, pg. 51)

Making your computer safe

If you want to start using your own computer again, then you need to buy anti-spyware software and run a full scan. If you don't have antivirus software on your PC then you should also install one of these products and run a full scan. Microsoft Essentials is available free of charge (see Appendix J: Security tools for victims, pg. 61).

Securing mobile phones

Always use a PIN

Activate your phone security settings so that after a minute of non-use, you have to put in a PIN before you can use the phone. Choose your PIN carefully, don't use your birthday, anniversary, child's birthday, 0123 or 9876 – they should be random numbers.

Mobile security software

Invest in mobile security software. It will prevent spam and virus software on your mobile. Most of them provide call blocking using whitelists. If you suspect that the perpetrator had access and could have put spyware on the mobile then you need to buy software to remove it (see Appendix J: Security tools for victims, pg. 61).

Call blocking

Use either the call blocking features in your mobile security software or buy an online app that offers call blocking using 'whitelists'. Call blocking using whitelists means that you can only be contacted by someone in your address book and all other calls will be blocked. There are options of what you can do with the blocked number such as send it directly to voicemail or hang-up.

Make sure you delete all contact numbers you have for your abuser and any other of his friends and family numbers that he may use to contact you.

Apps

Delete all apps that tell you where you are: maps, photos, check in, find my phone etc. You can reinstall the apps you want again later.

When installing apps pay close attention to what you are allowing them to do. If the app asks for administrator access, say no.

Understanding geolocation

Learn how to turn on and off your wi-fi, GPS and geolocation services, and change the default so that geotags aren't added to photos (see Geolocation, pg. 20).

Social networks

Block the perpetrator – even if he isn't on your friends list. Also block all his friends and family.

Be careful of adding any new friends. Perpetrators will often create fake e-mails and profiles of friends and family so you will add them to your friends list. Before you add a friend or family member just call or e-mail them to check they really sent you a friend invite. If he does use a fake profile block it immediately and inform friends and family on your friends list, asking them to block it as well.

Reduce your friends list. The more friends you have on your social network the easier it is for your abuser to find out information about you.

Change your privacy settings AND your security settings – see Appendix H: How to set Facebook's privacy settings to increase security, pg. 55.

Tell your family and friends. Stalkers not only stalk you, they will also contact and follow your friends and family via social networks. Let friends know that he may try to:

- contact them;
- send a friend request;
- create fake profiles to send friend requests;
- chat with them to try to find out more about you, or spread lies about you.

Ask friends to:

- block the abuser and his friends and family – if they won't do this, then you will need to remove them from your friends list;
- make sure that they have their privacy settings on friends only;
- not to post any contact details for you or respond to anyone who asks for them;
- not to post pictures of you or tag you in any photos (if they do, then remove the tags);
- let you know if the abuser contacts them or if he is using a fake profile.

Extra considerations for victims whose abuser has contact /access to children

Survivors who have children with their abusers may be put in the position where the child has e-mail contact or visitation with their father. The abuser can use that contact with their child to spy on their partner.

Mobile phones

Children, especially teens, can be smartphone users. As discussed previously, if the abuser has physical access to a phone they can put spyware on the child's phone and obtain information such as their location or even be able to listen to conversation via the mobile.

- Get a cheap pay-as-you-go phone for about £10 and insist that they use this when go on a visit. The mobiles that just call and text do not support spyware.

- If the child insists on taking his smart phone and is old enough, explain the risks of the abuser putting unwanted applications on their phone including ones with names like 'find my phone'.
- Put mobile security software on the child's phone (see Appendix J: Security tools for victims, pg. 61).
- Always use a PIN – as advised above, set up the phone so that the child has to use a PIN for the phone and SIM. If the abuser insists that the child unlocks the phone, then the phone should be immediately checked out for spyware.

Computers

An abuser may try to install spyware by e-mailing the child. If the child is using the same computer as the mother, the abuser will get access to all her information as well. If the child has their own computer it is still a risk to the mother because the child may post, e-mail or say something in a chat that gives away sensitive information about the mother.

There has been success in prohibiting a father from sending e-mails to their children because of this risk, but nevertheless:

- install anti-spyware software on any computer you or your children access;
- if the child is old enough, explain the risks and ask them not to open ANY file, picture, or joke from their father without talking to you first.

Social networks

Fathers may ask to keep in touch via a social network like Facebook. The risk for the mother is that the father asks questions or the child inadvertently provides the abuser with sensitive information. If the father is 'friends' with the child and they are also 'friends' with the mother then the father will be able to see some of the information about the mother.

If contact with the child via social networks can be avoided, it should be. If the child insists on contact via Facebook there is a slightly safer option.

The preferred option is that the child set-up a special Facebook account that **only has the father as a friend – no one else**.

The child should be educated what information they should and shouldn't have in their profile and what they can and can't post including photos (see Appendix F: Share cautiously, pg. 53). They should use the highest privacy and security settings (see Appendix H: How to set Facebook's privacy settings to increase security, pg. 55). The child should never accept files from the father because it could be spyware. On that special account they must also block their mother, her friends and relatives.

Stalking in the workplace

Abusers will use the same technology and techniques to abuse victims at work.

When stalking arises within the workplace, the relationship between victim and stalker is usually that of employer-employee, supervisor-employee, co-workers or service provider-customer (Mullen, Pathe and Purcell, 2009). Current or ex-partners may also try to harass victims at their place of work.

When victims are being stalked by work colleagues, they can be bombarded by text, e-mail, access the victim's computer or log in to the company network as the victim.

And because they are working in the same location there are also proximity issues such as bothering the victim at their desk, leaving notes/gifts, going through the victim's desk or possessions, and following the victim when they leave the office.

If the stalker is an employee, the company can take disciplinary action. The employer can also help gather evidence and provide supporting statements for victims. If necessary they can get a restraining order preventing the abuser from approaching or contacting the victim at work.

Risks

- **Physical danger.** Where they are both employees, the proximity of the stalker to the victim provides opportunities to physically attack the victim, or any colleagues that prevent access to the victim. If the perpetrator knows where the victim works, they will often also have knowledge of working patterns, location, and public information such as phone numbers.
- **Damage reputation.** Stalkers at work can easily spread gossip that can humiliate the victim or cause difficulties in their working relationships.

Clare Bernal

Clare Bernal, 22, was stalked by ex-boyfriend Michael Pech, 30, when she ended their three-week relationship.

On 14th September 2005 Clare Bernal was working in the Harvey Nichols store in London when Pech calmly approached her at the beauty counter.

Then in front of customers he walked behind the counter and shot Clare four times in the head with a semi-automatic Luger before killing himself.

Laura Black

Richard Farley a software engineer at ESL, became infatuated with Laura Black, 23, after a company function.

He stalked her at work in 1984. He was terminated from his employment in 1986 but continued to stalk Laura.

Black obtained a temporary restraining order against him on 2nd February, 1988, with a court date of 17th February, 1988 to make the order permanent.

This court date was a trigger and on 16th February 1988, Farley shot and killed seven people at ESL and wounded four others, including Black who was seriously wounded but survived. Farley was convicted of seven counts of murder in 1991.

- **Access to the victim.** Access to the victim's desk provides many opportunities to leave notes, gifts, use their phone or rifle through their drawers. Accessing their computer allows them to gather information, delete files, send out bogus e-mails from the victim's account etc.

Recommendations

Tell HR/Personnel

Victims can be reluctant to tell their employers. They are concerned about recriminations from colleagues, losing their job, being labelled as a trouble maker, or simply being embarrassed. However, it is vital that victims inform their employer that they are a victim of stalking. It will allow a company to take the necessary precautions to help protect the victim as well as other members of staff.

Have your calls screened

Have someone screen your phone calls so the stalker can't call your direct line or ask for you directly.

Be anonymous

Ask that your company e-mail address doesn't directly identify you – use a job title e.g. accounts@company. Do not have any presence on the company website, press releases, news letter etc.

Park safely

Ask for a parking space that is in plain sight of security or cameras, so that your stalker will be less likely to follow you or fit a GPS tracker on your car.

Protect your computer and phone

If you suspect that your stalker could be a work colleague then password protect your computer and log off or lock your screen whenever you leave it – even to get a cup of coffee. Also, make sure you have PIN access on your mobile phone so only you can use it.

Circulate photos

If you know your stalker is not an employee, then circulate a picture of him to reception, security guards and close work colleagues. Tell them that if he does come to your workplace, they must not allow him access to you, and ask them to call security or the police.

Workplace impact

“Of the 79% of stalking victims who had a job during the 12 months preceding the interview, about 1 in 8 lost time from work because of fear for their safety or to pursue activities such as obtaining a restraining order or testifying in court.

“Seven percent of victims lost time from work for activities such as changing a phone number, moving, or fixing or replacing damaged property. For 1 in 7 of these victims, a day or less was lost from work. More than half of victims lost five or more days from work.

“About 38% stalking victims reported that they had been fired from or asked to leave their jobs because of the stalking.”

(US Department of Justice, 2009).

Appendix A: Warning signs of a stalker

When your partner starts stalking

Over 50% of ex-partner stalking starts before the relationship ends (Mullen, Pathe and Purcell, 2009)

1. They become demanding/controlling, they want to know who you are texting and e-mailing, and what you are saying. They are suspicious, perhaps even paranoid.
2. They contact you multiple times a day asking you to confirm where you are.
3. They seem to know when you are at an unusual place – suspect that they have put some geo location software on your phone.
4. They start sending aggressive, abusive or threatening texts.
5. They start to contact your friends and family to check-up on you, get information about you, or to damage those relationships.
6. They start to spread rumours, put abusive, embarrassing comments online via social networks and/or forums.
7. They seem to know information that you haven't told them or know what you do online, such as websites you've visited, people you've chatted with or sent e-mails to etc. If so, suspect spyware on your computer.
8. Your passwords stop working or keep changing.
9. You find e-mails marked read that you haven't read, or e-mails sent from your account you haven't sent.
10. Money starts going missing from your online bank account or charges appear with online stores.
11. Information is deleted such as friend's contacts, computer files and e-mails.

When a stranger or acquaintance starts stalking

1. They start contacting you multiple times a day.
2. They are anxious to move from a dating site to private e-mail, texting, or telephone calls.
3. They keep asking for personal information such as where you work, where you went to school.
4. They agree with everything you say "as if you were soul mates".
5. They start talking about how much they like you only after a few chats.
6. They seem to be too interested, too soon.

7. If you block them they try contacting you using another different account.
8. They keep changing their story or somehow it just doesn't all add up. A good test is to tell a friend what he/she told you and get their response. They will be more objective.
9. They become demanding/controlling wanting to know who your friends are and why you haven't been online etc.
10. They know things about you that you didn't tell them.
11. They seem to know when and where you are online. They say "I know you were online because I saw your posts" or they are always showing up in the same chatroom.
12. They start adding your friends and family to their list, even though they don't know them.
13. They talk about you a lot in forums and elsewhere online. They make up stories about you or describe going on imaginary dates with you.

Appendix B: Key actions to reduce cyberstalking risks

For women whose partners force them to give them access to their phones, it may not be safe to hide your activities. In this case consider using public telephone boxes, a friend's phone or computers at your local library.

Mobile phone safety

1. Set your mobile so you have to use a PIN to unlock your phone. It should be set to lock after one or two minutes without use. Use random numbers – don't use birthdates or other guessable formats.
2. Don't use apps that tell you where friends are, or 'check you in'. If you suspect someone has put a tracking app on your mobile go through your apps and remove any suspicious ones.
3. Turn off geolocation services in camera apps and your mobile settings.
4. Get a cheap mobile to make sensitive calls or when you are going to a sensitive location.
5. Make sure that your phone is set to hide the caller ID.

Computer and online safety

1. Use a safe computer. Many victims' computers have had spyware/monitoring software installed. Use a different computer from a friend or library until you can install anti-spyware software on your computer (see Computer monitoring/spyware, pg. 24).
2. E-mail – get multiple new e-mail addresses. Make them anonymous; don't use your real name or nickname an ex-partner would recognise (see Appendix E: E-mail – creating new accounts, pg. 51).
3. Delete ALL online accounts. The most important thing you can do is delete ALL existing accounts – you don't know which accounts your stalker has access to. Create completely new, anonymous online profiles (e.g. on social networks, online shopping etc.) using your new e-mail addresses. Remember to change your security PIN with your mobile phone provider. **The only exception is if there is evidence such as abusive emails then don't delete that account** until the police have the information they need and tell you can.
4. Passwords – create completely new passwords. Abusers often get access to information because they know or guess a password. Don't use obvious security questions – most ex-partners can guess them (see Appendix D: Password security tips, pg. 48).
5. Set up several Google Alerts with your name, e-mail and phone number so if the abuser posts information about you online you will be alerted (see Appendix J: Security tools for victims, pg. 61).

6. Password protect your computer. At work always log off or lock the screen even if you are just stepping away for a few minutes. On a Windows machine you can lock the screen by holding down the [Windows] key and pressing L.

Social network safety

1. Social networks – these are not secure and your friends can easily leak information that can help an abuser track you down. If possible, deactivate (if things change you can reactivate it) your Facebook account and don't use it. If you want continue using Facebook then create a new account with an obscure name, use a fake photo and information. Only add your most trusted friends. Most of all make sure that you and your friends have put on the highest privacy and security settings.
2. Privacy settings – you need to use the most secure privacy settings to reduce information leaking out and feeding your stalker's obsession (see Appendix H: How to set Facebook's privacy settings to increase security, pg. 55).
3. Security settings – these are different from privacy settings and can help you identify if someone is hacking into your Facebook account (see Appendix G: Social networks – safety tips for stalking victims, pg. 54).
4. Explain to friends, family and co-workers that you are at risk and ask them to set their privacy settings to friends only. They should not accept people they don't know on their social network and ask them not to post photos, contact information or messages about you online. They should never give out your contact information to anyone. **They should always just forward the email, or take a phone number and say that you will call back.**

Appendix C: Gathering evidence

Preserve all online communications

- Save all text messages. Also, take a picture of the text message on the phone and save that to your computer in case you lose or damage your phone.
- Record all voice mail messages. Voicemail messages are deleted after a short while by the network so you should record all harassing voicemail messages. Make sure you note the exact time and date the voicemail arrived.
- Save all e-mails including all the header information (see below)
- Make a copy of all harassing messages/photos you find online in social networks/Chat/IM messages or conversations. On a Windows PC keyboard there is a special key that says 'Prt Sc' or 'PrintScreen'. If you hold down the 'ALT' key and press that special key, the PC will take a copy of what is on your screen. Open up a new Word or Paint document and paste the image in it, be sure to add the time and date of the conversation and save the file. As an extra precaution don't use an obvious name for the file like 'evidence' but something that the stalker wouldn't look in such as 'recipes'.

Log all harassment

Get a note book or create a document on your computer to log all incidents of harassment. Each time there are incidents write them down and **ALWAYS note the time and date of the incident.**

- If you are getting silent phone calls and/or hang-ups then write down every time that they occurred.
- If you suspect that they are accessing your accounts, write down if and when passwords have changed.
- If there is damage to your property, take a picture and note the date and time you noticed it.
- Take a picture of your stalker if he is following you, or showing up places that are unexpected.

Mobile phone logs

If you are getting high volumes of harassing calls or texts via your mobile phone, you can request that your mobile phone provider sends your mobile phone logs to the police. Your mobile phone provider will have to send the information directly to the police. You will need to be able to provide them with a crime number, name and contact details of your police force and a police contact name for your case. You will have to give your mobile phone provider formal permission to release this information.

The phone provider should be able to help you with this request. If they claim not to know of this procedure then ask them to contact the police liaison contact to help you with your request.

Until you get help from your mobile phone provider, write down all the relevant details in your harassment logs.

E-mail headers

Every e-mail that is sent includes some special information about the sender in the headers. So, even if they put a fake return address the police can often still track who actually sent the e-mail.

When you are printing off e-mails for evidence it is important that you show the headers when you print them off. Your e-mail provider help pages should explain how to reveal the headers. Go to their help pages and type in 'show headers'

For example in Microsoft Outlook you can right click on the e-mail and click 'options' to show the internet headers in a box where you can cut and paste them.

Association of Chief Police Officers (ACPO) guidance on making a harassment log

The following is guidance from ACPO on what should be included in a harassment log.

"It is important that you capture as much information and evidence as possible and below we have listed some typical examples of how you can help us by completing the log as fully and accurately as possible."

How to complete the log

- Start a new page for each incident.
- State the date and time of each incident.
- Describe in detail exactly what happened and how it happened:
 - Who did it and how do you know who they are?
 - What exactly did you see and hear?
 - What was said to you and by whom?
 - Was damage caused? If so, what and how?
 - How did it make you feel(were you emotional, angry, upset, frightened etc)?
 - Did anyone else witness the incident/behaviour? If they did then note their name, address and telephone number and any other details known to you, e.g. place of work.
- The person making the entry should sign, date and time each entry.

Please keep:

- phone texts and answer phone messages on landlines and mobile phones;
- relevant letters;
- video / photos;
- objects used in incidents;
- anything else which is relevant to the harassment or antisocial behaviour.

If you are not sure how to do this then ask the officer dealing with your situation."

Appendix D: Password security tips

- Create different passwords for different accounts. If the perpetrator doesn't have physical access to your home then you can write them down and store them in a secure place, or keep them in your purse or your wallet. Using password management software can make this much easier (see the section below How to store your passwords)
- Use passwords that aren't associated with you – ones that someone who knows you very well wouldn't be able to guess or figure out.
- If your e-mail or other account supplier has enhanced security features (such as sending alerts to a mobile phone as part of the password recovery process, or a requirement to type in the text from an SMS when you log in from somewhere unusual) then activate these features.
- If the perpetrator may have access to your computer don't use FireFox as a browser (because it can be asked to show all your saved passwords).
- If you are sharing a computer using Firefox then delete your passwords by going to the top of the browser, click Tools, Options, Security, and Saved Passwords; it will give you a list and you can delete the ones that concern you. Remember not to use the autosave option.
- If your abuser has access to your computer remember not to use the auto save option because then he can access the account.
- If you suspect your stalker may be someone at work, never leave your desk with your computer logged on.
- Never reply to e-mails claiming your 'account has been locked out'; it could be the perpetrator sending you a fake e-mail to get you to give away your password.

Password reuse is a common practice but creates a security risk

"Password re-use is a consequence of excessive number of passwords requested of users as multiple websites compete for scarce memory resources.

"In addition to decreasing the ability of users to employ strong passwords, it makes disparate sites' security interdependent as a password leaked at one site can be used at any other site where the user has registered it, particularly as most sites will use the same e-mail address to identify users.

"Attackers will rationally seek to extract passwords from the lowest-security websites and then re-use them at higher security websites."

(Joseph Bonneau Sören Preibusch, June 2010)

How to create secure passwords

- Use three random words run together e.g. 'cow & dandelion & rain', so the password would be: cowedandelionrain.
- Think of a quote or saying and remove all the vowels e.g. 'flat as a pancake' so the password would be: fltspncke.

- Try using a long, random sentence e.g. 'I love red shoes and pink handbags in the spring' so the password would be: iloveredshoesandpinkhandbagsinthespring.
- Or use the first letter of each word in a long sentence e.g. 'I love red shoes and pink handbags in the spring' yields the password: ilsaphits.
- Password recovery questions are not usually very good. People that know you may be able to guess your answer. Create a random answer for these questions e.g. if they ask your mother's maiden name use something like 'gorilla'. Remember, for most websites, these are not questions where you have to give a truthful answer; all you need to do is repeat the answer you originally gave them.

How to store your passwords

- If the stalker doesn't have access to your home (this won't work in an open environment like an office), you can write down the passwords or write a clue that will mean something to you such as S**B***. Try using an address book and file these clues under the website name. Put the address book out of sight.
- Password management software securely stores all your passwords and automatically fills in your password when you visit a website. You create a master password and then the software stores all your other passwords in an encrypted file.

Password managers

These are available for download at <http://download.cnet.com>:

- RoboForm
- Last Pass Password Manager
- Password Depot
- Password Prime

What not to do

- Don't use the name of your pets, children, dad, grandma or initials or use places where you lived or went to school, or your favourite colour, or your children's date of birth or your anniversary. Ex-partners know these facts and stalkers can use social networks and other online information to find out this type of information.
- Avoid simple passwords such as 1234, abcdefg, qwerty, password or your username
- Don't use the same password everywhere – if the stalker guesses the password on one account he will try it on others.
- Don't just change letters to numbers or symbols – they are easy to guess.
- Avoid websites which require truthful answers, for example your real date of birth, as part of the log-in process.
- Email providers have a problem when people take over accounts and change the passwords and the account recovery information to lock out the rightful owner. Some providers solve this problem by allowing the security questions to be reset to old values, but the abuser may be able to answer the old security questions – that's one the reasons that the advice we give is to set up new accounts from scratch rather than trying to hang onto old accounts.

Most common passwords that people regularly use on Gawker Media websites

- | | |
|----------------------|-------------------|
| 1. 123456 | 16. Sunshine 1234 |
| 2. Password | 17. Princess |
| 3. 12345678 | 18. Starwars |
| 4. (name of website) | 19. Whatever |
| 5. Qwerty | 20. Shadow |
| 6. Abc123 | 21. Cheese |
| 7. 111111 | 22. 123123 |
| 8. Monkey | 23. Nintendo |
| 9. 12345 | 24. Football |
| 10. 0 | 25. Computer |
| 11. Letmein | 26. F---you |
| 12. Trustno1 | 27. 654321 |
| 13. Dragon | 28. Blahblah |
| 14. 01234567 | 29. Passw0rd |
| 15. Iloveyou | |

Others include: children's & pet's name, hometown, date of birth, grandma, favourite colour, show or star etc.

(Source: Gawker media)

Appendix E: E-mail – creating new accounts

If the abuser knows the victim's personal e-mail address, simply blocking their e-mail account from contacting the victim is a good first step, but it is not likely to be enough. The abuser can constantly create new accounts to contact the victim.

Creating one or more new e-mail accounts:

1. Create one e-mail account for your most trusted contacts.
2. Create another account for when you register on websites.
3. Create a third e-mail account for financial accounts e.g. online banking etc.
4. Lastly, create one account for contacts that you and the abuser both know – they may give your new e-mail to the abuser.

Having multiple accounts is safer because if your abuser gets hold of one, the others remain safe. Managing multiple e-mail accounts does not need to be difficult. In most e-mail services' settings there are options to import e-mail from other accounts, even if they are from other service providers. For example, you may have a Hotmail account, a Yahoo! account, and an AOL account. By importing all your accounts into one service, you can easily manage them all from one spot.

Stay anonymous when creating new e-mail accounts

Unless an e-mail account is related to your professional life where you need to use your name, make your e-mail names anonymous so they do not identify you – not by name, birth date, age, location, ethnicity, work descriptor (like teacher, dancer) or other characteristic. It is also advisable not to create an e-mail name that is sexually suggestive, or expresses emotion.

Once you've created the new e-mail accounts, **check to be sure the service doesn't expose your real name as well**. To find out if your e-mail service displays your real name, send yourself an e-mail and check to see if your real name is displayed alongside your e-mail name in the sender field. Real names are displayed by default on e-mails you send from many of the major

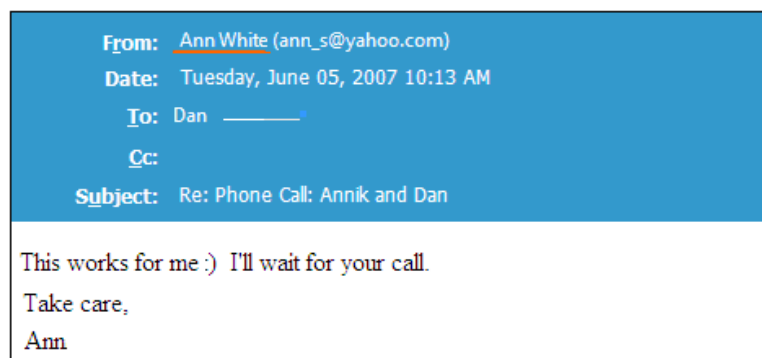
Security questions

Many sites ask you to answer a 'password hint' or 'security' question from a drop-down list. Unfortunately, many of the questions ask for answers that can be found in publicly available information such as your place of birth, a school you attended, or your mother's maiden name. In cases of domestic violence, chances are that your abuser will not only know these answers, but also know the correct answers to questions like the name of a favourite pet, your best friend in primary school, etc.

Answering any of these questions correctly could allow your abuser to get into, and take over, your account.

If none of the security questions allow you to give an answer that others couldn't discover, use a fake answer – just remember it! The service doesn't know if your answer is correct, it verifies only that you can repeat the answer you gave before. For example, what is your mother's maiden name? Purple Butterfly. Your first car? Green Butterfly. The city you were born in? Yellow Butterfly.

e-mail services. In the example below, you'll see how a woman who chose 'ann_s' as her e-mail name, also had her full name – Ann White – exposed.



NOTE: Other e-mail services have their own procedures for changing the display of your name in sent messages. If your e-mail service displays your name and you can't find how to hide this, e-mail your provider or search online for the proper procedure. If the provider doesn't allow you to hide your real name, use a different service.

Appendix F: Share cautiously

Sharing information online is all about considering two factors: what you are sharing (how sensitive the information is) and who you want to share the information with. If you give out general information or restrict it to only selected friends (who have their privacy restricted also), there is less risk in sharing it. However, if you say things that give away your location, where you work, or where you go out, then that information could leak out to your abuser.

Here are some categories of information you may want to consider as you determine what you're comfortable sharing or having others share about you publicly. This list isn't all the things you need to consider but is designed to get you to think about what information you give out and to whom.

Remember, even when you are careful to ensure that no individual blog or forum post contains information that gives you away, the accumulated information over time may do so. Periodically review the entire 'set' of information for risks, and delete anything that when combined is too much.

Information you should keep private:

- your name and the names of family members and friends;
- ages and genders - of you, your children, or other family members;
- identifying information: birth year, birth date, zodiac sign, city, schools, work or clubs;
- emotions. Abusers are probably very interested in whether you are happy or sad, or lonely, angry or feeling independent, have a new friend or are falling in love;
- addresses. This includes home and work addresses, as well as any other location you visit regularly. Consider what information should be exposed if you are announcing – or attending – an event for a birth, wedding, graduation, or death. Any event that the abuser could learn of and assume you will attend poses a real concern. Whether or not they 'attend' they may be watching and follow you home;
- phone numbers. This includes home, mobile phone, work number, and friends' numbers;
- personal numbers. Bank accounts, credit cards, debit cards, PINs, passport, birth date, wedding date, insurance policy numbers, car registration plate, NI number and more;
- information rich photos. A perfectly innocent photo can reveal more than you think. You might put yourself, family members, or friends at risk by posting photos that show where you go out or work, for example.

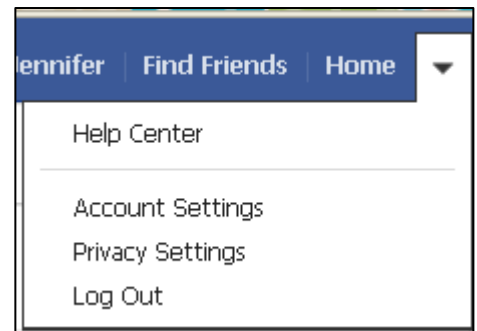
Appendix G: Social networks - safety tips for stalking victims

1. Create an anonymous user ID (nickname). Anyone can read a summary page for an ID.
 - a. Don't use your first and last name.
 - b. Don't post phone numbers.
 - c. Use at least two e-mail addresses – one for websites registration and one for personal use.
2. Block the abuser and any of their friends and family. Explicit blocking can provide stronger protection than just treating the abuser like any random stranger.
3. Use the privacy setting so only friends can see your profile. Go through all the options and tick each one individually. Don't allow tagging and disable search.
4. Don't use a password which the stalker can guess. Create a random password.
5. Don't add strangers or new friends on your 'friends list' unless you confirm that they are really who you think they are and not simply the stalker impersonating your friend.
6. Share cautiously – think carefully about what you post online. A friend could forward it to others or the abuser may be able to see posts on friend's wall.
 - a. Be careful about sharing personal contact information, location, talking about new relationships etc.
7. Delete comments/information – delete information or inflammatory comments on your wall that could provide the abuser important information or inflame the situation. If you need to vent, do it in private by calling or e-mailing a friend.
8. If the abuser posts harassing or threatening messages on your wall don't delete them and make sure you take a screen shot for evidence (see Appendix C: Gathering evidence, pg. 46).
9. Photos – don't post sexually suggestive pictures, or information about new partners – they could provoke your stalker. Also be aware that photos can provide clues where your stalker can find you e.g. at a favourite restaurant.
10. Don't let people take pictures on a mobile because they can be uploaded to the internet or distributed via e-mail. Those pictures could have a geolocation tag and the stalker can tell the exact location where the photo was taken.
11. Set your privacy settings so friends can't tag you in photos and untag yourself in any existing photos.
12. Disable search – go to Facebook/privacy/web apps/public search and disable the search option.
13. Check what your friends are posting/saying about you. Even if you are careful, they may not be.
14. Tell your friends that you are being stalked, educate them about the risk of your information getting to the stalker and ask that they block the stalker, their friends and family. Ask them to review their own privacy settings so it is limited to just 'friends'.

Appendix H: How to set Facebook's privacy settings to increase security

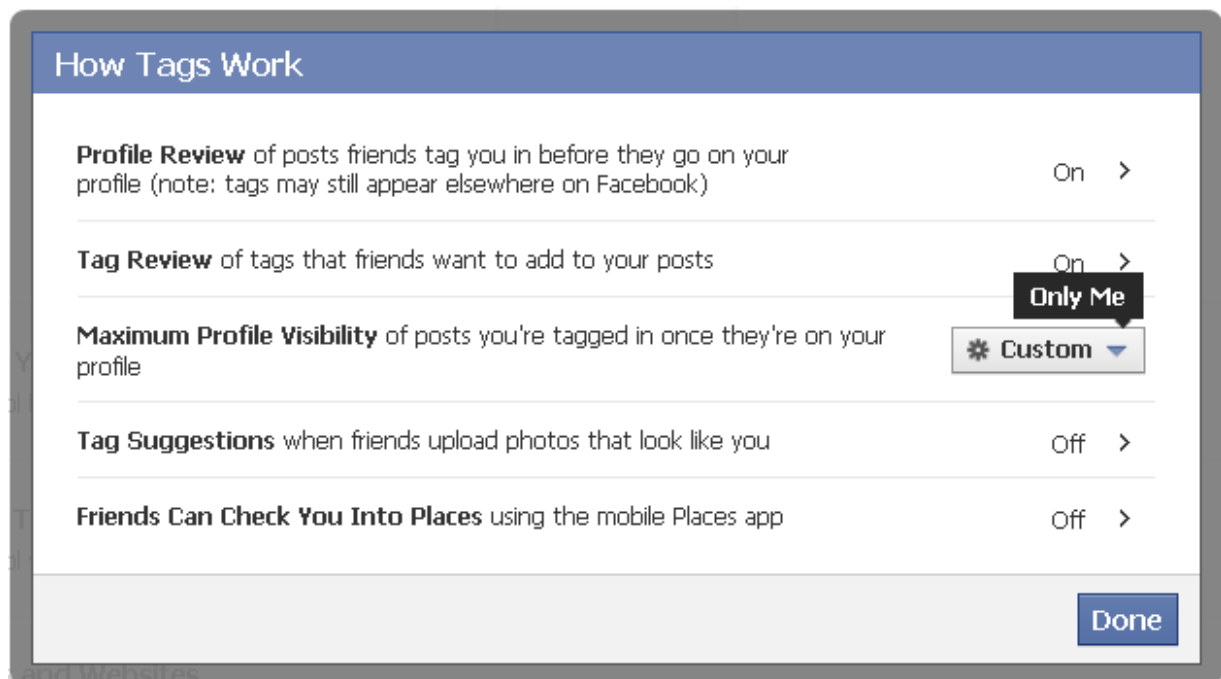
(October 2011)

The following section takes you step by step through Facebook privacy categories and what options users should select. Facebook Privacy settings can be found by clicking the arrow at the top right hand next to the home button.

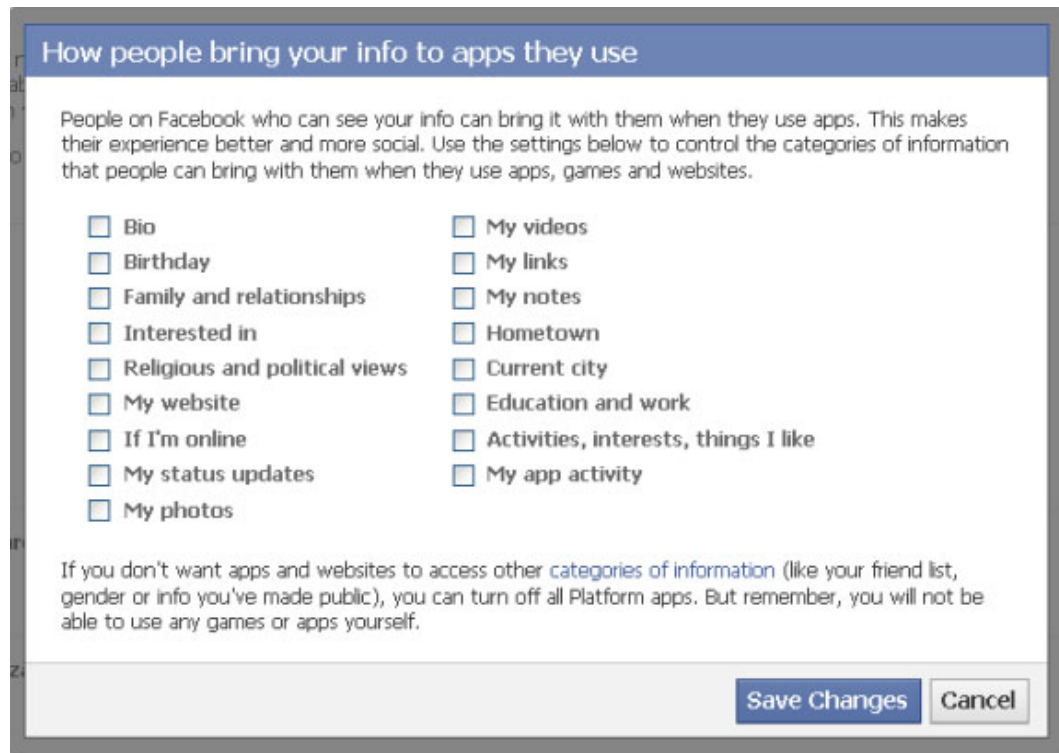


Step by step through Facebook Privacy Settings

1. **How You Connect.** The '**friends**' option should be used for all options in this category
2. **How Tags Work**
 - a. Profile Review - select '**on**'
 - b. Tag Review - select '**on**'
 - c. Maximum Profile Visibly - select '**custom**' then select '**only me**'
 - d. Tag Suggestions - select '**off**'
 - e. Friends Can Check You Into Places - select '**off**'



3. **Apps and Websites** – options
 - a. Apps you use – select '**Turn off all platform apps**'
 - b. Info accessible through your friends – **untick ALL boxes**



How people bring your info to apps they use

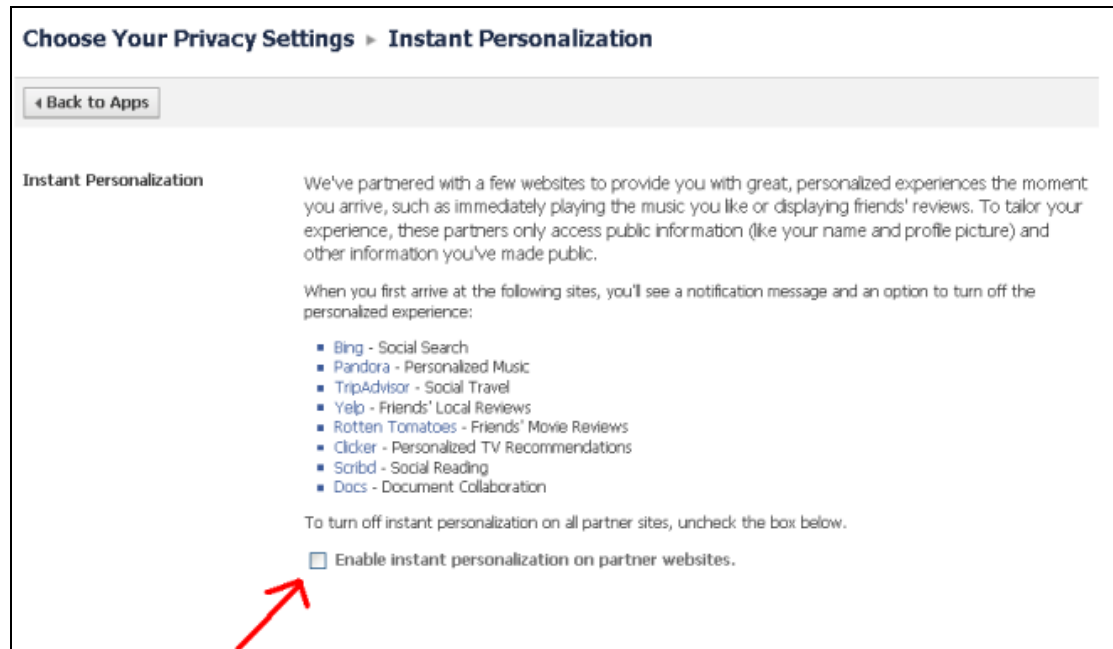
People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.

<input type="checkbox"/> Bio	<input type="checkbox"/> My videos
<input type="checkbox"/> Birthday	<input type="checkbox"/> My links
<input type="checkbox"/> Family and relationships	<input type="checkbox"/> My notes
<input type="checkbox"/> Interested in	<input type="checkbox"/> Hometown
<input type="checkbox"/> Religious and political views	<input type="checkbox"/> Current city
<input type="checkbox"/> My website	<input type="checkbox"/> Education and work
<input type="checkbox"/> If I'm online	<input type="checkbox"/> Activities, interests, things I like
<input type="checkbox"/> My status updates	<input type="checkbox"/> My app activity
<input type="checkbox"/> My photos	

If you don't want apps and websites to access other [categories of information](#) (like your friend list, gender or info you've made public), you can turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.

[Save Changes](#) [Cancel](#)

- c. Instant personalisation – **untick** 'Enable instant personalisation on partner websites'



Choose Your Privacy Settings > Instant Personalization

[Back to Apps](#)

Instant Personalization

We've partnered with a few websites to provide you with great, personalized experiences the moment you arrive, such as immediately playing the music you like or displaying friends' reviews. To tailor your experience, these partners only access public information (like your name and profile picture) and other information you've made public.

When you first arrive at the following sites, you'll see a notification message and an option to turn off the personalized experience:

- Bing - Social Search
- Pandora - Personalized Music
- TripAdvisor - Social Travel
- Yelp - Friends' Local Reviews
- Rotten Tomatoes - Friends' Movie Reviews
- Clicker - Personalized TV Recommendations
- Scribd - Social Reading
- Docs - Document Collaboration

To turn off instant personalization on all partner sites, uncheck the box below.

☒ Enable instant personalization on partner websites.

- d. Public search – click on edit and then **untick** 'Enable public search'
4. **Limit the audience for past posts** – if you have followed the recommended changes above there is no need to change this setting.

5. **Blocked people and apps** – One of the most powerful features that users should take advantage of is the ability to block other users. You should block the perpetrator and all known associates immediately – even if it is a new account. You should also ask everyone on your 'friends list' to also block the perpetrator and known associates.

Victims and friends need to be aware the perpetrator may try to 'friend' them using a different account. If that happens they should also block the new account.

The person being blocked does not know they have been blocked.

Blocked applications such as games can leak information to others. If there are applications with the account they should be blocked. If users are sent invites to games, calendars and other apps they should not accept or use them.

What happens when you block someone?

A block prevents specific people from viewing your profile (timeline). Any ties you currently have with the people you block will be broken (friendship connections, friend details, etc.). Your profile (timeline) will not be visible to them and you will not appear in their search results or friend lists. Blocking is mutual, so they will also become invisible to you as well.

Keep in mind that blocking someone may not prevent all communications, such as interactions in third-party applications, and does not extend to elsewhere on the internet.

(Facebook, October 2011)

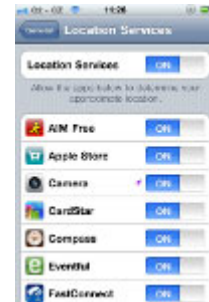
Appendix I: Disabling mobile pictures' geotags

Source: www.icanstalku.com

iPhone (iOS 4.x)

Apple greatly simplified the way to turn off location services on a per-application basis.

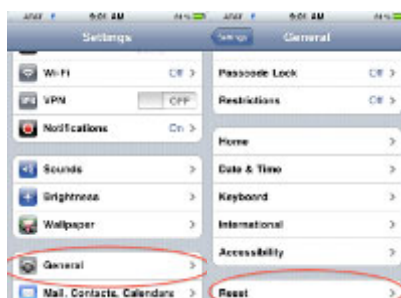
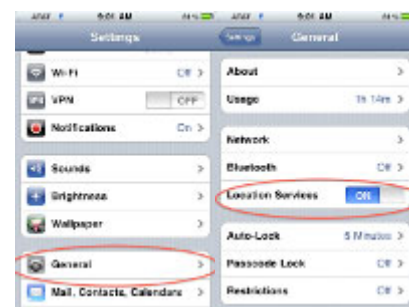
To see your settings, go to Settings, General, then Location Services. From there you can set which applications can access your GPS coordinates or disable it entirely.



iPhone (iOS 3.x)

With the iOS 3.x there are two ways to disable geotagging of photos. The first involves disabling of all location based services. To disable this feature go to Settings, General then set Location Services to off.

Be warned: This will turn off ALL location based services for ALL applications. Of course you may still wish to use location based services for other applications (such as maps and driving directions).

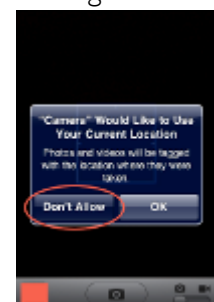
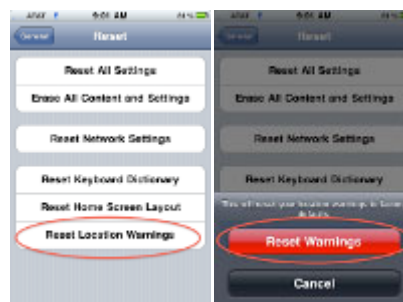


There is no easy way to disable location based services for just one application. However, we can make the iPhone prompt us at first use for each application. Once reset, the first time we enter the application we can enable or disable location based services for the application. To do so we need to go to Settings, General, Reset.

Warnings, and then Reset Warnings. This restores all of our location based warnings for each application to the default, which in most cases is 'ask on first use'.

From here, once we enter into the default camera app on the iPhone, we can select Don't Allow. This will prevent the camera app from geotagging our photos.

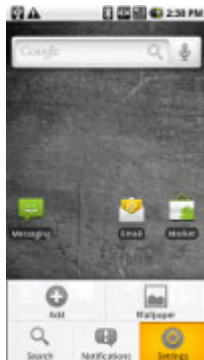
Be careful here! We want to select Reset Location



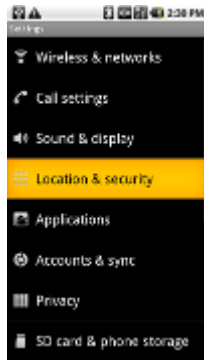
Google Android

As with the iPhone, there are two ways to turn off geotagging. To completely disable GPS location finding for all applications, we will need to do the following:

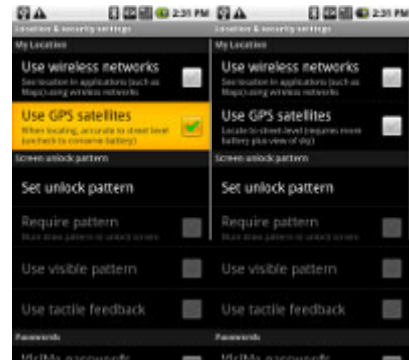
Step 1: Press the Menu Key and then Settings



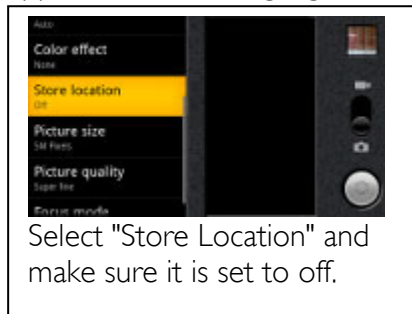
Step 2: Press Location and security



Step 3: By default, GPS is on. Uncheck it to turn it off



Just as with disabling the GPS in the iPhone, this will break location based information for all applications, including legitimate uses.



Select "Store Location" and make sure it is set to off.

In order to disable geotagging for just the camera application, start the camera app to make sure that you are not saving your location. This is the menu on the left side of the camera application; it slides out from left to right.

Once this is disabled, the camera app will no longer add geotags to your images.

BlackBerry devices

There are multiple ways to disable the geotags on a BlackBerry. We detail three ways here:

1. First option – this will disable all GPS capabilities on the phone.
 - a. Select 'Options'
 - b. 'Advanced Options'
 - c. Select 'GPS'
 - d. Press 'Menu' key
 - e. Select 'Disable GPS' and select 'Yes' to confirm
2. Second option – disable application permissions.
 - a. Select 'Options'
 - b. Select 'Security'

- c. Select 'Applications Permissions'
- d. Select 'Edit' on the application (default is 'Prompt' for BlackBerry Core)
- e. Expand 'Connections'
- f. Change 'Location' (GPS) to 'Deny' or you can disable within the application

Most apps i.e. Google Maps, Facebook Places etc. will default everything to 'allow' to give apps permission regardless of app settings chosen during setup.

3. Third Option – Disable geotags on your pictures via the camera settings.
 - a. Go into picture-taking mode (via HomeScreen, click icon 'Camera')
 - b. Press the 'Menu' button and choose 'Options'
 - c. Set the 'Geotagging' setting to be 'Disabled'
 - d. Finally, save the updated settings

Appendix J: Security tools for victims

All victims should get advice on home and personal security.

Google Alerts

Google Alerts are free. You can set up an alert with key words such as your name, e-mail and phone number. When any of those appear on the internet Google will e-mail you an alert. You could also do alerts for your stalkers name and e-mail to see if there are comments about you but that do not necessarily use your name. Note that you only receive alerts for new mentions; to check existing mentions you will need to do a Google search.

When you set up an alert use quote marks around names, numbers and e-mails to get more accurate results e.g. 'firstname lastname' or 'youre-mail@xyz.com'

To set up an alert go to: www.google.com/alerts

Anti-spyware

All stalking victims should install anti-spyware on their computers. Anti-virus software is NOT the same. You need specific software that will look for spyware/monitoring software. The following are some respected software providers of anti-spyware products.

Trusted Anti-Spyware

www.2-spyware.com	Reviews
www.malwarebytes.org	£19.95
www.pctools.com (spyware doctor)	£29.99
www.superantispyware.com/	\$29.95
www.webroot.com (spysweeper)	\$39.99
Microsoft windows defender	Free
(http://windows.microsoft.com/en-US/windows7/products/features/windows-defender)	

Anti-virus

Anti-spyware doesn't replace anti-virus software and everyone should also use an anti-virus software product. There are numerous products to choose from. Microsoft provides a free anti-virus product called Microsoft Essentials. You can download it at www.microsoft.com/download/en/details.aspx?id=5201.

Password managers (available for download at <http://download.cnet.com>)

RoboForm
Last Pass Password Manager
Password Depot
Password Prime

USB memory stick

Use a USB memory stick to store a back-up copy of your important documents and evidence so that if your abuser does access your computer or if your computer gets damaged you won't lose them. Keep a copy of your friend's email addresses and phone numbers here so if, for example, your account does get broken into and the online address book is deleted you will not lose touch with your friends.

Mobile phone apps

There are thousands of apps. Some can be useful – if you put in 'Hide My Text' into a search you will find apps that take incoming texts and hide them in a special app so they don't show up in your text messages app. This could be useful to keep more sensitive messages out of immediate view.

Voice recorder

Buy a small hand held voice recorder so you can record threatening phone conversations or voice mail messages.

Paper shredder

Use a paper shredder to get rid of any sensitive documents. Perpetrators will go through trash and recycling bins to find information.

Register with CIFAS (UK's Fraud Prevention Service)

CIFAS Protective Registration is a service that enables individuals to seek protection against possible impersonation/identity theft. When someone checks your credit (for example to get a store card) they will see that your name has been marked by CIFAS and that they will require additional information to prevent someone else using your information for the a card or loan.

Appendix K: Support Organisations

National Stalking Helpline

Website: www.stalkinghelpline.org

0808 802 0300

Women's Aid

Website: www.womensaid.org.uk

Freephone 24 Hour National Domestic Violence Helpline: 0808 2000 247 (run in partnership with Refuge)

Scottish Women's Aid

Website: www.scottishwomensaid.org.uk

Telephone: 0800 027 1234

Welsh Women's Aid

Website: www.welshwomensaid.org

Telephone 0808 80 10 800

Women's Aid Federation Northern Ireland

Website: www.womensaidni.org

Telephone: 0800 917 1414

Refuge

Website: www.refuge.org.uk

Freephone 24 Hour National Domestic Violence Helpline: 0808 2000 247 (run in partnership with Refuge)

National Centre for Domestic Violence

Website: www.ncdv.co.uk

Telephone: 0844 8044 999

Mobile: Text NCDV to 60777

Men's Advice Line – support for male victims of domestic violence and abuse

Website: www.mensadvice.org.uk

Telephone: 0808 801 0327

Rights of Women – educating and empowering women on their legal rights

Website: www.rightsofwomen.org.uk

Legal helpline: 020 7251 6577

Sexual violence helpline: 020 7251 8887

Samaritans – 24-hour confidential emotional support for anyone in a crisis

Website: www.samaritans.org.uk

Helpline: 08457 909 090 Ireland helpline: 1850 609 090

Technology glossary

administrator: the most powerful form of user account, which allows the widest range of operations to be performed, including installing software and changing settings.

Android ®: the smartphone operating system developed by Google. It is used by on a variety of mobile phones and tablets.

anti-virus: software designed to detect viruses (and possibly worms and trojans), which may commonly have been delivered through visiting web pages, receiving e-mails and downloading software. Sometimes known as 'scanning' or 'disinfecting' a computer.

anti-spyware: software designed to detect spyware.

apps, applications (see also platform app): accessories which can be downloaded to a smartphone, tablet or computer, or used in conjunction with a social networking site, which provide a specific additional function.

BlackBerry: a brand of smartphone specialising in secure messaging.

blacklist: a list of names (typically web sites, e-mail addresses or phone numbers) which are prevented from communicating with a particular device or user. See whitelist.

blog: abbreviation for web LOG. A website which is a personal journal of comments and opinions.

Bluetooth®: a technology designed to allow wireless communication between devices that are close together. For example, linking your mobile phone to a headset.

call blocking: a service supplied by a phone company or as an application, to blacklist callers.

CIFAS: anti-fraud organisation with a Protective Registration scheme for people at risk of impersonation.

cloud: the collection of applications, services and data storage available through an internet connection. The physical location of the provider is generally unknown, and may consist of multiple servers in many countries.

cookies: small packages of data stored by a web browser at the request of a website, and used to recognise you when you return to that site later.

coarse location: the position of a device obtained by reference to nearby mobile phone base stations and wi-fi hotspots. The accuracy is typically from within a few hundred metres to over a kilometre.

CSV: comma-separated values, a simple document format where the elements are separated by commas.

digitally assisted stalking: stalking activity which is enhanced or accelerated by the use of digital technology such as mobile phones, computers and internet.

digital footprint: the information about you available online. Includes personal, financial information, your internet usage, your location, friends and much more.

e-mail: electronic mail.

e-mail header: information sent along with an e-mail which contains information about the sender and the delivery process.

Essentials (Microsoft): a free anti-virus program

exif tags: see metadata.

Facebook (see also Wall, Places, Profile, Friends): the most popular social networking site.

fine location: the position (latitude and longitude) of a device, determined by a GPS receiver.

Firefox: a popular web browser.

Friends (Facebook): the list of people who you have agreed to share the most information with.

geotags: see metadata.

geolocation: geographic location. Using technology to determine and record the position of a computer or phone, or where a photo was taken.

Google Alerts: a free service that sends e-mail updates of the most recent Google search results, based on words specified when each alert is set up.

Google Earth: a 3D mapping and photo library site. Photos are uploaded through the Panoramio sister site.

Gmail: e-mail service provided by Google.

Google Maps (see also Latitude): a mapping and driving directions website that also includes satellite imaging and ground-level photography (Streetview).

GPS: Global Positioning System, a global satellite-based location system that provides accurate location and time information.

GSM, 3G, 4G: three currently (or soon to be) deployed generations of mobile phone technology (GSM also known as 2G). GSM is designed mainly for voice and SMS

Hotmail: a free e-mail service provided by Microsoft.

hotspot: a wi-fi base station, either inside a home or office for private use, or provided to the public commercially – free of charge or by subscription.

identity theft: the act of fraudulently impersonating someone, using credit card details or other information such the full name, date of birth, current address or previous addresses to get goods or credit in the victim's name. The impersonator might also post damaging information online in order to harass the victim or the victim's colleagues and acquaintances.

Latitude (Google): a social networking feature which allows users to share the details of their latest location on a Google map.

IOS: Apple's operating system for their iPhone and iPad devices.

iPhone, iPad: Apple's smartphone and tablet devices.

instant messaging (IM): is text-based communication between two or more users over the internet. Unlike e-mail or text, IM happens in real time.

IP address: internet protocol address. A number associated with an internet connection, which historically was unique to each connected device but today may also be shared. For most domestic internet connections, the IP address very easily determines the internet service provider (ISP), but only the ISP has the means to identify the premises served or the mobile device in use. However, IP addresses in logs and e-mail headers are useful as evidence.

location services (see also fine/coarse location): facilities available in a mobile device, or within the cloud, which can determine a device's location, and make it available to an application.

log: list of transactions made between a user and a website or other internet site.

malware: any form of MALicious softWARE which has bad intentions. Can include spyware, viruses, trojans and worms.

meta data: hidden pieces of information attached to a website (as meta tags) or photograph (as exif tags or geotags), revealing specific properties such as the author's name, type of camera and settings used, or location of the photo.

operating system: software which defines a device's personality and user interface, on top of which applications are installed. Examples include Windows, Android and IOS.

Panoramio: photo library website specialising in urban and rural landscapes.

PDF: portable document format, a commonly used standard for document publication and interchange.

PIN: personal identification number, a numeric password, often 4 digits; used to unlock a mobile phone, access online accounts or validate card transactions.

Places (Facebook): an application which allows the user to register and share their location.

platform app (Facebook): applications which are integrated into Facebook and can be given permission to read and write users' data.

profile (social networking): biographical information associated with an account holder.

privacy settings: parameters which can be set within a social network site to determine which other users, including non-members, are allowed to see information which has been posted.

regional location: a concept in iPhone 4 where applications can be alerted to the user entering within a large (>half a kilometer) pre-defined radius.

root[ing]: the process of unofficially obtaining administrator access to a device, esp. an Android phone, often by exploiting a security weakness in the device.

RTF: rich text format, a popular form of Microsoft text document.

search (social networking): allowing the content and profile from a social network to be found by public online searches e.g. Google.

security settings: a menu within a social network site or web browser which allows to user to choose an appropriate balance between safety and visibility.

SIM (SIM card): a chip-card which contains the subscription details of a mobile phone account.

social engineering: using deception to obtain information or persuade people to perform unauthorised acts.

social network: a website whose users are bound together by a common interest or desire to share information.

Smartphone: a phone that has an operating system that offers more features. They enable people not only to talk and text but e-mail, use social media, surf the net, play games and pay bills. They can hold your music, video and photos. Of course they also hold important data about us such as our contact information, diary, passwords etc.

SMS/text message: a message of up to 160 characters that may be sent between phones, or other devices with phone technology installed.

spoof: to masquerade or impersonate, often the sender of a communication (e-mail address or phone number).

spyware: software that secretly snoops information from a phone or computer and sends it to a third party.

SSL: Secure Sockets Layer. An encryption technology intended to make web browsing more secure.

status (social networking): a short and topical autobiographical posting.

tag (Facebook): annotating a photograph to indicate a person is pictured within.

tablet: a hand-held touch-screen computer

trojan: a form of virus, which is not self-propagating, but is contained within an innocent-looking e-mail or application.

virus: software buried within an otherwise legitimate object, such as an e-mail or application, which has an unwanted and often undesirable effect upon the computer. It will normally have a mechanism within it to propagate to other computers from the infected one.

Wall (Facebook): a section of the Facebook website where users post and share content with others.

whitelist: a list of names (typically web sites or e-mail addresses) which are specifically allowed to communicate with a particular device or user. See blacklist.

worm: a form of virus where the self-propagation is the prime motive.

wi-fi: a wireless networking technology that allows devices to connect to each other over a range of a few hundred metres. It is commonly built into laptop computers, tablets and smartphones.

Yahoo!: a large and popular website, including facilities for search, free e-mail, instant messaging and subject-based discussion groups.

Bibliography

ACPO Homicide Working Group (2003). *Findings from the Multi-agency Domestic Violence Murder Reviews in London*. Metropolitan Police.

Boberg, M (2008). Mobile phone and Identity: A Comparative Study of the Representations of Mobile Phone among French and Finnish Adolescents. *Academic Dissertation, University of Joensuu* .

Dinei Florêncio and Cormac Herley (2007). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, (pp. pages 657-666). New York, NY USA.

Garfinkel and Cox (Feb 2009). *Finding and Archiving the Internet Footprint*. Presented at the first Digital Lives Research Conference. London, UK: Naval Postgraduate School.

Joseph Bonneau Sören Preibusch *The password thicket: technical and market failures in human authentication on the web*. (WEIS - The Ninth Workshop on the Economics of Information Security, 2010).

Ling, R (January 2001). "It is 'in.' It doesn't matter if you need it or not, just that you have it." *Fashion and the domestication of the mobile telephone among teens in Norway*. At the conference: "Il corpo umano tra tecnologie, comunicazione e moda" (The human body between technologies, communication and fashion). Triennale di Milano.

Lookout (August 2011). *Mobile Security Mobile Threat Report*.

Maple, Short and Brown (2011). *Cyberstalking in the United Kingdom, An analysis of the Echo Pilot*. University of Bedfordshire. National Centre for Cyberstalking Research.

Mullen, Pathe and Purcell (2009). *Stalkers and their Victims*. Cambridge University Press.

OFCOM (April 2010). *Assessment of Mobile Location Technology* .

OFCOM (August 2011). *The Communications Market*.

OFCOM (April 2011). *UK Adults' Media Literacy Report* .

Thomas M Evans PHD, J Reid Meloy PHD (2010). Identifying and Classifying Juvenile Stalking Behavior. *Journal of Forensic Science* .

UK Home Office (Jan 2011). *Homicides, Firearm Offences and Intimate Violence 2009/10*.

US Department of Justice (2009). *National Crime Victimization Survey - Stalking Victimization in the United States*.



© Network for Surviving Stalking and Women's Aid Federation of England, 2012
ISBN: 978 0 907817 52 9

Network for Surviving Stalking

PO Box 88
Lydney
GL15 9AG
Telephone: 07501 752741
E-mail: info@nss.org.uk
Website: www.nss.org.uk

Network for Surviving Stalking is a registered charity and company limited by guarantee
Registered Charity No: 1088762
Company No: 6913845
Registered Office: 6 Telford Crescent, Reading, RG5 4QT

Women's Aid

PO Box 391
Bristol
BS99 7WS
Telephone: 0117 944 4411
Fax: 0117 9241703

E-mail: info@womensaid.org.uk

Websites: www.womensaid.org.uk www.thehideout.org.uk

0808 2000 247: National Domestic Violence Helpline (run in partnership between Women's Aid and Refuge)

Women's Aid Federation of England is a registered charity and company limited by guarantee
Registered Charity No: 1054154
Company No: 3171880
Registered Office: Kings House, Orchard Street, Bristol, BS1 5EH
VAT Registration No: 850 5437 31