

Internet Safety for Victims of Violence

If you are reading this, chances are you have been the victim of violence where the threat of re-offence is significant. Or you know, or work with, such victims. For you, the internet can provide greater safety and a wealth of resources, but it can also hold additional risks.

A few simple changes to your online actions will greatly increase your safety. The following guidelines cannot guarantee to keep you from harm, but they will help you learn how to take additional precautions to better protect your anonymity, location, and identity.

Two caveats:

- Technology advances rapidly. To be sure you have the latest advice, look for more safety information through the online resources listed at the end of this booklet, or through the nearest domestic violence agency in your area.
- This is written primarily for victims who have escaped a violent situation, but also contains advice for those living in a violent relationship. If you are still in a violent relationship, the [Assume monitoring](#) section will be of particular importance.

In this document...

- About abusers
- Preparing to leave
 - Assume monitoring
 - Protecting children
 - Create new, anonymous accounts
- Once you've left
 - Prevent tracking
 - Safer Socializing
 - Information in photos
 - Cell phone smarts
 - Anonymous e-shopping
 - Finding trusted resources and getting help

Let me start by saying you do not have to have a degree in computer science to dramatically improve your online safety. Consistently applying a few simple skills and staying vigilant will do a lot to help you stay safer.

About Abusers

There are four primary forms of abuse - emotional abuse, financial abuse, reputational abuse, and physical abuse of people or property. If you are the victim of relationship violence, the abuse may include all of these forms.

It is likely that you know your abuser, they may be a family member, have a charming as well as a violent side, and they may be very adept at bullying people, gaining sympathy, or telling a good story to get what they want - which if you are in hiding, will be information on how to find you.

Your abuser may not be particularly savvy about technology, but they don't have to be to successfully employ many methods of finding you. Setting up a new profile that includes the city in which you live, exposing your friends list, blogging about what you're doing, leaving an 'away' message on your email saying where you'll be for work or vacation; these are all things the abuser might be able to discover. And, it may not be you that exposes your whereabouts, someone else may accidentally do it for you. Not only do you need to learn to hide information, but anyone who knows where you are needs to learn how to keep your information private.

Preparing to leave:

The decision to leave an abuser isn't an easy one, and as you seek information and assistance in doing so, you may be at considerable risk. Technology can provide strong support for anyone leaving an abusive situation; it can also provide strong tools to help an abuser track you. Understanding how to stay safer online as you prepare to leave can help reduce the risk your abuser discovers what you are planning, and make fleeing easier.

Assume monitoring



Abusers track the online activities of those they abuse, and your best bet is to accept this and plan accordingly. Trying to 'clean' the computer of spying, tracking or parental control tools being used to monitor you, or changing your passwords, will only alert the abuser, increase their suspicion, and potentially increase the threat to your physical safety. Similarly, deleting your browser history files to trying to hide which websites you've visited is likely to backfire. Unless you are computer savvy, it's hard to fully erase these search results and simply finding an empty history file may set off an abuser.

Learn more about spyware under the section [Prevent Tracking - clean your computers, mobile phones, and vehicles](#).

You will be far safer using a computer outside your home, and outside your abusers sphere of influence for any activities related to finding shelters or getting help. Consider using a computer at work, a library, a community center, or trusted friend or family member's home.

Hidden Cameras



You should assume that hidden video cameras have been installed to listen in on any conversations you may have either in person or via the phone, to watch for actions like packing a suitcase, or to see purchases like a lock, or gun, etc.

Phone monitoring

A phone with a cord is more difficult to tap than a cordless phone or cell phone, but whether or not the phone itself is tapped, you should assume that hidden video cameras will pick up anything you say inside your home. You should also assume that any calls made while standing in your yard, or any call from your cell phone could be tapped or monitored.



Your cell phone may have location (GPS) tracking functionality, and your abuser may use this to monitor everywhere you go. This tracking functionality can be turned off - for help, just go into your carrier's store and ask them to turn it off, or search for instructions online - but turning this off may enrage your abuser or let them know you're onto their actions. It's best to simply leave that cell phone behind when you flee so that you cannot be traced this way.

To avoid having your calls detected, you have a couple of options. You can use a prepaid phone card from a public phone, call from a trusted friend's home, or purchase your own cell phone. (See the section - [Cell phone smarts](#) - for more information). If you choose to purchase a cell phone, it is critical that the phone is not found.

Protecting children



Many of you will flee with children or teens who have online lives of their own. If your children know in advance that you are preparing to leave, it is vital that they understand how to protect this information. They need to understand that monitoring tools may be in place within your home and yard, and online via computer, game consoles, and cell phones and that anything they say or do may alert the abuser to your family's plans.

Once you have left the abusive situation, children and teens will also need to adhere to the safety guidelines outlined in the rest of this booklet. Like you, they will need to be especially cautious about sharing any information about themselves. Abusers will use their friends, or leverage the parents of their friends, or the friends of their friends to gain information. It is a particularly heavy burden for youth to bear as it requires constant vigilance against sharing things most teens routinely share - what they're doing, where they are, how they're feeling, who they're hanging out with, etc.

You will need to ensure that your children not only understand the risks, but also master the skills needed to successfully protect themselves and your family while interacting online. It's important to acknowledge that isolation is part of abuse, and that reconnecting may be part of healing.

Create new, anonymous accounts



To start fresh online without being monitored by an abuser requires that you create *new accounts on unmonitored computers*.

Creating new accounts on a computer that is monitored by your abuser means the accounts would be compromised from the outset as the abuser would know about them through any computer monitoring they are doing and MAY INCREASE your risk of violence.

Similarly, using existing accounts on a computer that is not monitored by your abuser can place you at risk of monitoring. For example, parental control tools monitor a user's email account, regardless of the computer or phone the email was sent from.

Never access your new, anonymous accounts from a computer or cell phone that may be tracked by your abuser.

Start by creating new anonymous accounts for email and browsing. To ensure your privacy make sure you only use a computer that you know is not being monitored by your abuser. (See the section - [Email - Create a new account](#) - for how to do this). Be sure you use strong passwords that have nothing to do with your life. See the section [Strong passwords are critical](#) to learn more.



In your new email account, create a contact list that includes the names, email accounts, phone numbers, and emergency numbers for your safe contacts so you have this information at hand should you need to flee without warning. Use this email for all messages you do not want seen by your abuser.

Send yourself emails (from this account, to this account) containing any information you will need after you've left - this may include snapshots of what is in shared bank accounts, or documentation of other assets, anything related to medical care, photos you want to keep, anything you may want, but won't be able to go back and access once you've gone into hiding.

Open a new, private bank account at a different bank. Do NOT transfer funds from an existing account to this account as anyone with access to the old account can see where the transferred funds were sent. Instead, keep it anonymous by taking cash out of the old account, or having a cashier's check made out in your name. Then take the funds to your new bank and make the deposit into your new account.

See the section [Finding trusted resources and getting help](#) to identify organizations and content that can help you through this process.

Once you've left:

Staying safe once you've left your abuser requires you to closely guard your privacy. Most shelters do not require you to provide your real name or other identifying information, and at least until you understand how information is protected, using a pseudonym is a wise precaution.

Prevent Tracking - clean your computers, mobile phones, and vehicles



If your abuser had access to your computer or home, they may have placed tracking, monitoring, or spying software on your computer, laptop, handheld device, or mobile phone. The tracking method may be in the form of a specialized spying product that has been secretly installed, or it could be that they have turned on "parental controls" making you the 'child' account so that everything you do is reported to them. No one has to be a technology genius to use either of these options.

Even if you don't think your devices have been compromised, your safest bet is to assume they have been, and that everything you do or say online, including your passwords, calendar, email, and contacts, is being monitored until you have cleaned these devices. Trust your instincts. If you believe you are being monitored through your computer, you probably are - even if you can't find the monitoring software on your computer. If you aren't technically savvy, you may want to have a TRUSTED friend or family member help you, or, for a relatively low cost you can use a company to do this for you. Be sure to have your friend or the company also look for any parental control tools/settings (as the abuser may have set up the parental controls to monitor you as a 'child') and have them look for unique spying applications, and do this for *all* of your devices. Sometimes it can be nearly impossible to get spyware off your computer, and transferring files from the tracked computer may bring the spyware onto your new computer.

Next, if you do not have up-to-date security software installed, do so now. If cost is an issue, use one of the excellent free alternatives (search online for "best free security software" and look for recent reviews on credible sites like CNET or PC Magazine). Set the security software to automatically update so your machines have the best protection possible. Do NOT leave your computer unprotected, this is like leaving your front door unlocked.

Make sure your firewall, and wireless connection if you are using one, are password protected with new, strong passwords. (See the section on safe passwords to learn how).

Once your device(s) are clean and secure, Create new, strong passwords for your administrator accounts and be sure you are the only person with access. Set a password to log on to your computers and phones so that no one can use them.

Do not skip these safety steps. If your machine is forwarding all your information to your abuser, the safety steps outlined in the rest of this material cannot help you.

Once you've accomplished these steps you can be reasonably confident that your online actions aren't monitored, and your safety has significantly increased.

Check your vehicle



If you own a vehicle, take one more precaution and have it checked for any hidden GPS tracking device. Tracking devices are cheap to purchase, and provide the abuser with a data stream of wherever the vehicle - and you -

goes.

The cheapest option is to search every nook and cranny of your vehicle for something that looks out of the ordinary, particularly any kind of wire or electrical device that has been installed in an odd place or is attached magnetically. On bicycles and motorcycles this is fairly straightforward, but if you have a car, it becomes more complex - especially if the person has had access to the inside of your vehicle. If you know cars well, inspect it inside and out, on the engine, behind the bumpers, and on the undercarriage, even look behind the dashboard. If you aren't car savvy, you may want to take it into a shop where they can give the car a more thorough inspection.

You can purchase a GPS bug detector from spy equipment or home security websites or stores for around \$400 to \$500 USD. These work by detecting frequencies used by transmitting devices. A domestic violence shelter in your area may have one you can borrow.

Safer Socializing

Building a support network is critical to anyone who has experienced physical or emotional trauma, and the internet provides great opportunities to find this kind of support, and have it available 24 hours a day. It's hard to call family, friends, counselors or supporters in the middle of the night when grief, panic, or anger strikes, but someone is probably online. Using forums or searching for information can happen at any hour. You just need to do so safely.

This section contains information about how you can stay safer when using various internet services that enable socializing.

Email - Create a new account



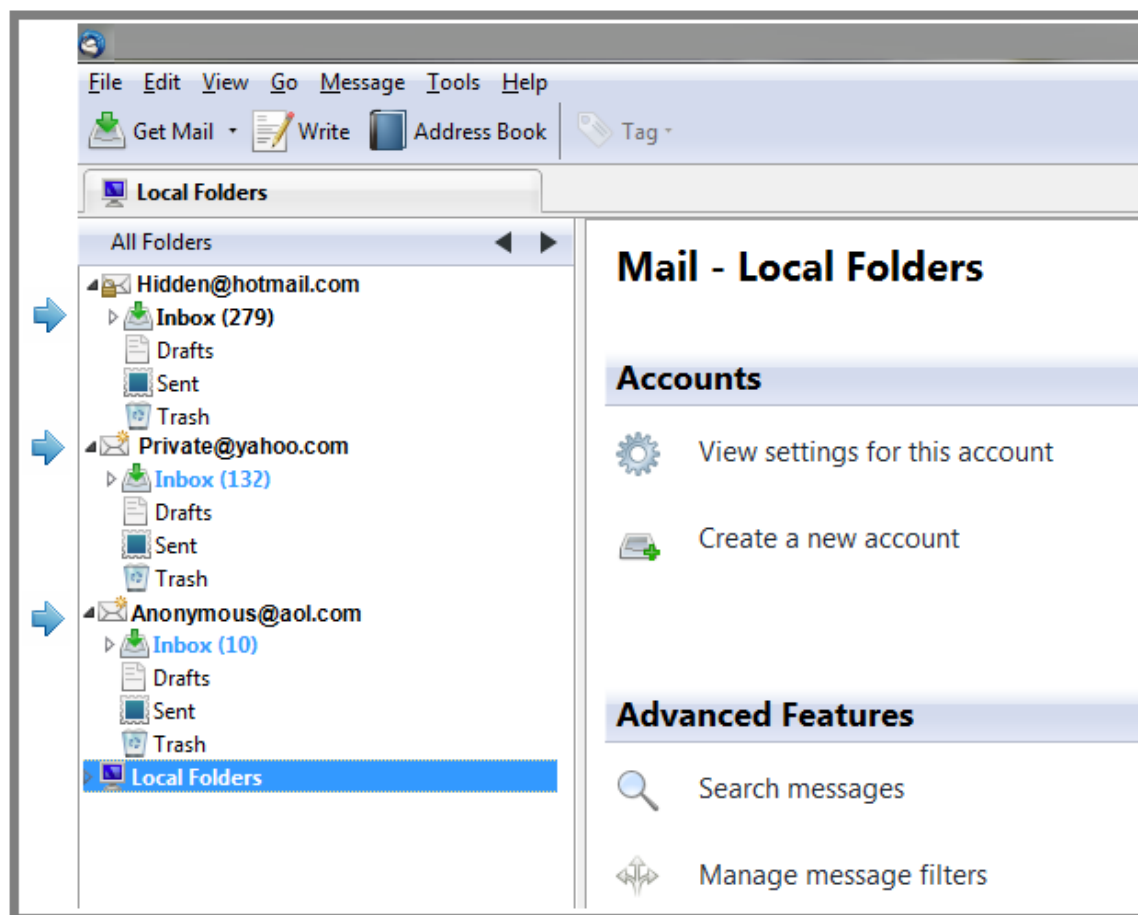
If your abuser knows your personal email address, simply blocking their email account from contacting yours is a good first step, but it is not likely to be enough. They can constantly create new accounts to use to contact you.

Consider creating one or more new email accounts, they are free and easy to set up. For example:

1. Create one email account for your most trusted contacts.
2. Another account for interactions with people you only know from online sources.
3. A third for financial accounts e.g. online banking or PayPal.
4. Lastly create a unique account for contacts that you and the abuser both know - they may be sympathetic to giving your new email to the abuser.

Having multiple accounts is safer because if your abuser gets hold of one, the others remain safe. Managing multiple email accounts does not need to be difficult. In most email services' settings you will find an option to import email 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.

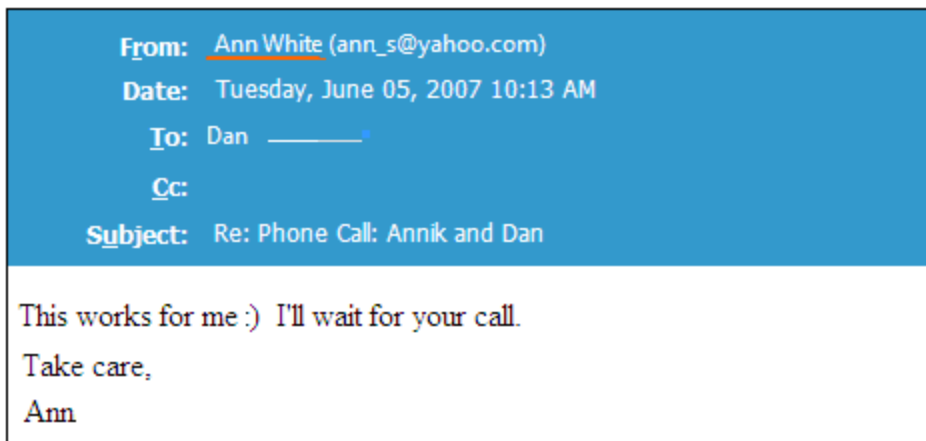
By importing all your accounts into one service, you can easily manage them from one spot. The illustration below shows how you can see multiple accounts through your primary email account.



Stay anonymous when creating new email accounts

Unless an email account is related to your professional life where you need to use your name, make your email aliases anonymous so they do not identify you - not by name, birth date, age, location, ethnicity, work descriptor (like teacher, dancer..) or other characteristic.

Once you've created anonymous email accounts, check to be sure the service doesn't expose your real name. To find out if your email service displays your real name, send yourself an email and check to see if your real name is displayed alongside your alias in the sender field. Real names are displayed by default on e-mails you send from many of the major e-mail services. In the example below, you'll see how a woman who chose "ann_s" as her alias, also had her full name - Ann White - exposed.



The good news is that you can change the setting to hide your real name. Below are the instructions for doing this in Windows Live (Hotmail ,MSN mail).

1. In Windows Live, click the *Options* button on the right side of the screen (next to the Help icon with a question mark on it)
2. Click *View and Edit Your Personal Information*
3. Click *Settings* on the left side of the screen
4. Click on *Profiles* under Account Information
5. Click *Edit Your Account Profile*
6. On the Account Profile page, either delete your first and/or last name or replace them with information that doesn't identify you personally. You can use any alphanumeric characters (A-Z; 0-9) and any of the special characters on your keyboard except for ;, <, >, ,, (,), ", \$, and !.

NOTE: Other e-mail services have their own procedures for changing the display of your name in sent messages. If your email 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.

Keep your email private

There are two aspects to keeping your email private: how strong your passwords are, and **who you share your email address with**. Protect your email accounts by carefully considering with whom, and which sites, you choose to share this information. You want to be able to contact, and be contacted by, those who support you, and avoid letting your account information fall into your abusers hands.

Strong passwords are critical



If you lived with the abuser, or they had access to your computer at some point in time, you should assume that any passwords you have were compromised. Change them all once you are safely away.

Reminder: If you are still living with your abuser, changing passwords can place you at risk. This advice is only for those who have left, or have created entirely new identities that are not accessed from any device that could be monitored.

Safe passwords don't have to be hard to create; they just have to be hard to guess.

Creating a strong password, changing a password, or using multiple passwords makes many people anxious because they believe it requires memorizing multiple complex passwords, such as Wts4e_79#PBa3*.

This isn't the case. Here's what you need to know to make strong and memorable passwords.

Safe Password ground rules:

- Use unique passwords for each site so that, if one password is compromised, all of your Web sites and information isn't exposed.
- Passwords that are short, simple words or include numbers that relate to personal information (such as birth date, address, pets names) are easy to guess. So are sequences like 123456 or abcdef. Don't use them.

Logic	Password
Use a familiar phrase typed with a variation of capitalization and numbers instead of words (text message shorthand).	<ul style="list-style-type: none"> • L8r_L8rNot2day = Later, later, not today • 2BorNot2B_ThatIsThe? = To be or not to be, that is the question. • ROFL!Cn'tStOp = Rolling on the Floor laughing! Can't Stop
Create a system. Perhaps it begins with the first four letters of a website, then a standard pattern. - maybe the pattern is - 1!2@3#	<ul style="list-style-type: none"> • Amaz1!2@3# = Amazon1!2@3# • Chas1!2@3# = Chase (your bank)1!2@3#
Create a password from an easy to remember phrase that describes what you're doing, with key letters replaced by numbers or symbols.	<ul style="list-style-type: none"> • 1mlook1ng@hotmail = I'm looking at Hotmail (We replaced the ls with 1s., and the word at with @)) • MyWork@HomeNeverEnds

<p>Spell a word (with at a minimum of 8 characters) backwards with at least one letter representing a character or number.</p>	<ul style="list-style-type: none"> • \$lidoffaD = Daffodils (The \$ replaces the s.) • y1frettuB = Butterfly (The 1 replaces the l.)
<p>Use patterns from your keyboard. (See image below) Make your keyboard a palette and make any shape you want.</p>	<ul style="list-style-type: none"> • 1QAZSDRFBHU8 is really just making a W on your keyboard. • xdr5thnbvcx creates a pyramid



It's okay to keep a list of your passwords, just be sure to first change the existing passwords and put the new list in a safe place that's not near your computer.

Avoid security questions with publicly available answers

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 or partner 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 favorite pet, your best friend in elementary 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 give the answer that you provided again if you forget your password. For example,

what is your mothers maiden name? Purple Butterfly. Your first car? Purple butterfly. The city you were born in? Purple Butterfly.

Change your existing accounts' security questions/answers. Not only do you need to protect new accounts, you need to protect your existing accounts.

Avoid Away messages

Lastly, consider any "away" or "out-of-office" messages you might leave on your work or personal email accounts. Do not let these reveal where you will be going. If an abuser sees your going to be at a conference for work, or on holiday in a specific location, it won't be hard for them to show up at your location, or to use the opportunity while you are away to break into your home.

IM - Create a new account



If you use Instant Messaging (IM), use your new email account(s) to create a new IM account. When setting up the account, be sure to choose a nickname/user name that does not identify you. Do not use identifiable information in your URL (your website address). Do not use your own photo or any photo that could be uniquely associated with you, and don't indicate your location. Set your account settings to be private (friends only) and be selective in your choice of friends so that your abuser does not have access through a friend's login. If you choose the privacy option that allows friends of friends to see your account, your abuser may be able to see your information through a mutual friend.

Social Networking sites and Forums



Social sites that allow you to share and get support are important tools for victims of abuse, but they must be used carefully. Used carelessly, they can lead the abuser to your new door, workplace, or other location.

Stop using existing accounts

You may want to continue to check these accounts periodically, but do not post any new information. If your abuser is aware of these accounts, they will continue to monitor them to glean information. If you want to continue using an existing social networking site or forum, create a new private account to avoid being identified or tracked by an abuser.

The illustration below helps you see how information is exposed on 'private' sites. 'Jessica' set her MySpace account to be private. Yet, look at how much information is still exposed. We see her name, her photo, her comment, her age and location, when she last logged in (indicates whether she is still active on the account) and her URL further exposes her name. As any of this information is updated the abuser has the opportunity to learn more.

Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds

Jessica

"This Is ME....Take it or leave it :)"









Female
23 years old
CONCRETE,
Washington
United States

Last Login:
7/27/2007

This profile is set to private. This user must add you as a friend to see his/her profile.

Contacting Jessica

 Send Message	 Forward to Friend
 Add to Friends	 Add to Favorites
 Instant Message	 Block User
 Add to Group	 Rank User

MySpace URL:
http://www.myspace.com/j_massing

Before joining a new forum or social site, monitor it anonymously for a while. Get a feel for what it will take for you to successfully and safely use the site. Look at the site's privacy settings and policies, do they respect your privacy and do they make it easy for you to notify them of any problems? If the site doesn't provide strong privacy settings, pick a different site.

Look for how well the site is moderated - do they quickly crack down on abusers? How much information is available about users who's sites are set to 'private'? Can you search on their name and find them? Can you see a basic profile? Though she set her site to 'private', Jessica is entirely exposed.

Blogging and Micro-blogging



If you want to use a blogging, or micro-blogging site (like Twitter), these are designed to be public, you can't make them private. You must be especially diligent about how sharing as information adds up over time. Sensitive information regarding your location, activities, or emotions, should never be provided.

Location tracking

Social networks like Facebook and Twitter have implemented location functionality that, if turned on, shows exactly where you are whenever you post. Location information can be dangerous for anyone to share, however for victims this information can be life threatening. Be sure that any location functionality in any online service you use is OFF. (This includes shutting off Bluetooth functions on mobile devices.)

Creating new accounts is easy

With a few simple guidelines you'll be able to create an anonymous account.

- Omit any information that can identify you. In general, only fill in required fields, and, if these fields can be seen or used in a search, use fictive information about location, date of birth, etc.
- Only use profile photos that do not identify you. No photos of yourself, pets, kids, homes, etc.
- Carefully select your privacy settings to be sure you are not visible or searchable to anyone you have not expressly said you want contact with
- Only invite **trusted** people to join you - when in doubt, leave someone out.

Share cautiously

You can share a great deal of information about your feelings, experiences, hopes, fears, and more without ever mentioning your name, age, location, vocation, etc. However, remaining anonymous and sharing publicly without exposing too much information is a critical skill for you to practice, and requires consistent vigilance. Before starting, watch a few users and see how much you learn about the ways people expose their emotions, reference places they've been or events they are attending, etc.

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 the information is general in nature or restricted to only selected friends, who also have strong privacy settings, there is less risk in sharing it. However, if you include information that identifies you, your possessions, or location in some way, carefully limit access or the information could be shared with your abuser.

Sensitive information

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 is not a definitive inventory of identifying information, but it can get you thinking about what you share and with whom you share it.

- 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, school, state, county, hobbies, clubs, or workplace
- Emotions: Abusers are usually 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, phone calling card, Social Security Number, passport, driver's license number, birth date, wedding date, insurance policy numbers, loan numbers, VIN numbers, license plate numbers, 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 live or work, for example.

Remember, even when you are careful to ensure that no one 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.

Others may be sharing information about you

You aren't the only one sharing information about you. Use a browser to search for information others have posted, and consider these possible sources:



Family and friends

Family and friends may post information about you in blogs, on genealogy sites, and on photo-sharing sites, for example. They may announce events that the abuser can attend or monitor.

In the example below, a young girl created a very safe social networking profile that had no information about herself - yet in just three comments by friends, she is totally exposed - full name, phone number, birth date and year, location, where she goes to school, and where to find her.

None of these friends acted maliciously, yet they completely exposed critical information.

Do You Expose Others? Do they expose you?

<p>ChrisInSpringfield</p> 	<p>7/16/2006 5:37 PM</p> <p>Hey, Happy Birthday Blanche!!! 16 and driving - ouuuuu Yeah! i am not getting my cell back until saturday, is your home # 555-1212? Leave me a message w/ directions to the party on your site...</p>
<p>Tisha</p> 	<p>7/16/2006 5:37 PM</p> <p>darn O'connelly, you're growing up! Happy b-day! The party's @ Tucson bowling rite? Hey Maria, cool glasses.</p>
 <p>SexySantoros</p>	<p>7/14/2006 9:29PM</p> <p>Blanche DAhling, happy early b-day! We're going to be in Taos this weekend, so can't come to the party let's meet at the game Monday - GO Chargers! Check out my new glasses.....</p>

Employers

Employers may share information about you on the company's website. If you are working in a big company, you may also want to be cautious about how much is visible to other employees on

an intranet. When you attend a conference, be sure your name is not exposed on an attendee list on the conference website or documents. If you are a speaker, you may need to take extreme caution when arriving and while at the conference to never be alone, and when leaving to be sure you are not followed, and recheck to be sure a GPS tracking device has not been hidden on your car. You may want to explain to your employer that "I really like my privacy, please don't place any information about me on the web."

Schools

Be sure any school you attend does not expose your information on their Web sites. This may be in the form of a student directory at universities or colleges or it may be through photos and captions, listings of sports team members, event dates, awards, etc. This information may be about you, or one of your children - either way, you become locatable.

The illustration below shows how universities often expose information about students. With many

universities anyone can type in the name of a student and see their phone number, address, email account, and what they are studying. You don't have to have any affiliation with the school, or provide login credentials to find students.

The screenshot shows the 'INFORMATION TECHNOLOGY THE UNIVERSITY OF UTAH' website. At the top, there is a search bar with the text 'campus: a to z index | map | calendar' and a 'Search' button. Below the search bar is a navigation menu with letters A through T. The main content area is titled 'Campus Directory' and contains a search form. The search form has the text 'I am searching for...' and a search box containing 'john smith'. There are radio buttons for 'Employee', 'Student' (selected), and 'Department/Organization'. A 'GO' button is next to the search box. Below the search form, there is a 'Back to Search Results' link. The search results for 'john smith' are displayed in a table-like format:

Name	Smith, John Jacob
Major & Degree Sought	Economics MS
Email	john.smith@utah.edu
Phone	801-828-7■■■
Address	Smith, John Jacob 123 NW APT 2■■■ GROVE, UT 84062

On the right side of the page, there is a sidebar with links for 'Emergency Info', 'Directory Info', 'U Colleges, Departments & Organizations (PDF)', 'Search Tips & FAQs', 'Abbreviations List', 'Update directory listing?', and 'Campus Operator 801.581.7200'. At the bottom of the page, there is a footer with the text: 'OFFICE OF INFORMATION TECHNOLOGY, 101 WASATCH DR. #201, SALT LAKE CITY, UT 84112 | 801.581.7022 ©2009 THE UNIVERSITY OF UTAH | WEBMASTER | DISCLAIMER | PRIVACY'.

Information in photos



Photos and videos often share far more information that people realize, and while this information can increase anyone's risks, it can be particularly jeopardizing to victims of violence.

What you see in an image you post may be that the photo really flatters you. What an abuser sees may be considerably more. To understand this, look at the

photo below that was posted on a young girl's social networking site.

The house number tells me she lives on a corner. Her profile tells me the city she lives in. Using Google Street View, I can virtually cruise down 1st street until I see a house that looks like this and know exactly where she lives. With this information, I can look at the property records, learn her parents identities, how much the home is worth, and the floor plan of the home. Her location also indicates which school she is likely to attend so I could find her there as well.

This home would not be that hard to break into, the windows next to the door are single pane glass, and another view of her hoe shows the rest of the windows are the old sliding kind that if you jiggle hard will slip past the locked position. But there is no need to break in because where they hide the spare key is obvious. That planter on the steps is broken on the side - why? because it is lifted often. And so on.

Now that you know how to really look at a photo, practice this skill of seeing all the "hidden" information in images by looking at a lot of photos posted online. Next, look at videos people have posted. What else do they add? Voice, mannerisms, friends?

If you are posting photos or video to a private site that is only seen by your closest, trusted friends, you run little added risk - they already know where you are, and how you're feeling etc.



But before you post a photo on a site that can be seen by more than your closest, trusted friends, consider *each piece of information* the picture provides to understand if it will increase your vulnerability.

Note: There is a lot of other information to be found in this photo, that is worth understanding:

I look at this girl, she's cute and looks friendly, like she wants friends. I see her general age, and can identify her on the street. I see that she's not entirely comfortable being photographed by her stiff posture and smile. From her pose you see that she isn't super self confident - this isn't a "look at me" pose of a girl with hair back, chest forward, screaming to the world she thinks she's hot.

She doesn't have any friends in the photo, which may mean that she's more of a loner. This girl isn't Goth, she's not a cheerleader, she's a nice, sweet teen and a little sporty.

Her family's economic bracket is lower middle class based on the home and her clothes. She isn't wearing designer clothes, doesn't have an expensive hair cut, and isn't wearing jewelry.

Cell phone smarts



It is hard to imagine how we managed before mobile phones. These mini-computers help us keep in touch, find information, make purchases, provide entertainment, find destinations, and stay safer.

Cell phones also provide opportunities for abusers to continue their exploitation, and for individuals themselves to struggle over selecting the most private options. Your safety depends partly on the choices you make when using a cellphone.

Following a few simple guidelines will help you and your families have safer mobile experiences.

The safest cell phone is one that cannot be traced back to you

Abusers are often very good at creating convincing stories for companies about why they need your contact and location information and 'helpful' staff may provide it. If the company does not have your information, they cannot expose it.

Purchase a phone without a service contract whenever possible so you don't have to show ID, give your name or address. You may also consider buying a used phone off a classified ads site that won't be traceable back to you. **Note:** If you do need to show ID, consider having a friend purchase the phone with their ID. Or, weigh the pros and cons of showing your ID at the specific location you are making your purchase from. For example, you wouldn't want to show ID at a store where your abuser has a friend, or use a carrier that the abuser works for, but if there is no real way for the abuser to know where you purchased the phone, showing your ID may not be a significant risk.

Then, use prepaid phone cards so you don't have any billing relationship to a mobile service provider that can be exposed.

Protect your phone number. Abusers will try to contact and locate you through other people if they cannot contact or locate you directly. Insist that the people you entrust your phone number with do not share it. You may want to consider using more than one SIM card so you can use different phone numbers for the types of people you contact.

Applying safety precautions requires understanding the features of the phone and the service you choose. Before you buy a phone for yourself or your child, ask: What are the features on the phone, and what services do these features enable? Look at the answers from a safety perspective: What safeguards are in place with these features?

Cell phone features

- Does the phone or device have Internet access? If so, it is critical that nothing you post online from your phone identifies you or your location.
- Is the phone or device Bluetooth enabled? Blue-tooth is a technology that allows a mobile phone to seek, discover and 'talk' to other Bluetooth-enabled devices in the area. This means

that you may receive unwanted content or your information might be accessed without permission. At the very least, set your phone to 'not discoverable' using your Bluetooth setup menu, or if not using Bluetooth, just turn it off.

- Does the phone or device have location (GPS) capability? GPS can be a lifesaving tool if it allows a *trusted* contact to see if you have been abducted. That said, *extreme caution* should be used if you are considering a location service that allows friends or strangers to track your location, learn your patterns, and expose you, or your property, to privacy invasions or physical harm. Strictly limit the number of people who have access to this information.
- Does the phone have a camera? Review every single image for identifiers before sharing them electronically, once you've sent these, you have no control over where they end up. Does the image include a building, landmark, or scene that might indicate where to locate you? Would seeing the image excite, enrage, or enthrall the abuser? If you want to share the image(s) printing these, or showing people who are physically present these photos on your phone is a better option.
- Can the phone access chatrooms or social networks? If so, can you consistently protect your safety when communicating from your phone?
- Does the phone or service allow you to hide your number from being displayed in Caller ID? Does the service allow you to block certain numbers from calling you? You may also want to consider designating your phone as a 'child phone' where you can restrict the numbers that call you to a specific list of numbers. This way, an abuser can't reach you by simply using new phones each time.

• **NOTE:** If the cost of purchasing a new or used phone is an issue, many domestic violence and safe shelters can provide you with a donated phone.

Anonymous e-shopping



When e-shopping, using classified ads, or online auction sites, ensuring your continued privacy is key. If there is any chance that your abuser knows your existing accounts, passwords, favorite stores, or favorite sellers, close your accounts and create new ones.

Don't be tempted to keep an existing account where you've earned a strong reputation as a buyer or seller, it is better to start over than risk being discovered.

Use a new email account with a secure password when setting up new e-commerce accounts. Provide only the minimum required information to create the account, and use an alias rather than your real name or information as your abuser may be looking for new accounts with elements of your real information.

Create a new payment account

Once you've created new accounts for buying and selling, you need to be sure you aren't tracked through the actual purchase process. Close any existing PayPal or similar accounts and create new ones that hide your identity and use strong passwords.

You should have already changed your credit card numbers, changed banks, and established a new bank account so that you are financially untraceable. If you haven't, do so now. Reminder: Only make these changes if you have left your abuser. If you are still with your abuser, making changes. **Note:** This is only the case if you have left your abuser, do not change these if you are still with the abuser.

Keep your true address hidden

Your physical location may be your most sensitive information. If you have relocated and are keeping your location secret, have any online purchases delivered to the address of a friend, of a shelter if they will accept packages on your behalf, or to a new post office box in a location that will not be familiar to your abuser. Your safety is worth the added hassle of picking up your packages elsewhere. Remember, if the seller doesn't know your true identity or address, they can't inadvertently disclose this to your abuser.

Finding trusted resources and getting help

Remember, only seek help on a computer or phone that is not under the control of your abuser. This includes assuming a video camera is recording any conversations, calls, visits, or actions taken within a home shared with an abuser.

To find information about the specific resources in your area, search for domestic violence help in your town, county, or state, or leverage the resources of one of the following national organizations.

National Domestic Violence and Human Trafficking Resources

1. **[National Domestic Violence Hotline](http://www.ndvh.org/)** (<http://www.ndvh.org/>) or call 1-800-799-SAFE (7233) or 1-800-787-3224 (TTY) – This is a crisis intervention and referral phone line for victims of domestic violence. The service also has an email address and access for the deaf. Hotline staff members can speak in English or Spanish and have access to translators for many other languages.
 - **[Get help in your area](http://www.ndvh.org/get-help/help-in-your-area/)** (<http://www.ndvh.org/get-help/help-in-your-area/>) To find out more information about domestic violence in your state, call, write, or email one of the state coalitions listed.
 - There are additional handouts on spyware and technology safety for victims at: www.nnedv.org/safetynetdocs
2. **Relocation Counseling and Identity Protection Initiative**
 - The Safety Net Technology Project at the National Network to End Domestic Violence partners with Valenda Applegarth at Greater Boston Legal Services to provide national assistance to victim advocates and attorneys who are helping victims relocate and/or protect your privacy. If you need some specialized assistance, please have your victim advocate or attorney reach out for technology information at: www.nnedv.org/contact.html

3. [National Coalition Against Domestic Violence](http://www.ncadv.org/) (http://www.ncadv.org/)
 - [State Coalition List](#) – Lists the phone numbers for the state offices of the NCADV. These offices can help you find local support or a shelter from domestic violence, as well as free or low-cost legal services. (National Coalition Against Domestic Violence)
 - Download a document showing [address confidentiality programs in states across the country](#) (<http://www.ncadv.org/files/AddressConfidentialityProgramsintheUnitedStatesforwebsite.doc>)

These types of programs allow individuals who have experienced domestic violence, sexual assault, stalking or other types of crime to receive mail at a confidential address, while keeping their actual address undisclosed. Rules and eligibility vary from state to state.
4. [Polaris' National Human Trafficking Hotline](http://www.polarisproject.org/content/view/90/95/) (http://www.polarisproject.org/content/view/90/95/)
 - The NHTRC is a national, 24-hour, toll-free, anti-trafficking hotline operated and implemented by Polaris Project and funded by the Department of Health and Human Services (HHS). The NHTRC works to improve the national response to protect victims of human trafficking in the U.S. The NHTRC also works in collaboration with the anti-trafficking movement in the United States, which includes: HHS Rescue and Restore Coalitions, DOJ-funded Human Trafficking Task Forces, FBI Innocence Lost Task forces, Federal victims' services and outreach grantees, statewide human trafficking task forces, and community-based initiatives.
 - **NHTRC Hotline Services:**
 - a. Call 1-888-3737-888 to report a tip; to connect with anti-trafficking services in your area; or to request training and technical assistance, general information, or specific anti-trafficking resources.

Taking the advice provided here will keep you safer, though it cannot guarantee to keep you safe from all harm.

This resource material is brought to you by Linda Criddle, a leading expert on internet safety, and President of LOOKBOTHWAYS Inc. More information about internet safety can be found on www.ilookbothways.com