What others say can give away important information

Family and friends may post information about you in blogs, on genealogy sites, and on photo-sharing sites, for example. You may not want people to know you were fired or your mobile number or how you were out partying. But this is the type of information friends post about you. A stalker will also make comments to get your friends to reveal information about you.

Employees

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.

Students

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

Photos and videos often share far more information that people realise. What an abuser sees may be considerably more than you do. They will look in the background for clues – have you moved, who is that with you, when you go out, where do you go etc. You and your friends need to make sure photos online don't compromise your safety or cause your abuser to escalate his actions.

Using mobile phones safely

It is hard to imagine how we managed before mobile phones. They also can help an abuse trace or harass you. The safest mobile phone is one that cannot be traced back to you – pay as you go phone. 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. Get a pay as you go phone because these do not require a contract so you don't have to show ID, give your name or address. 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.

Consider some of these features before you get a new phone

- 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 location might be accessed without permission. 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.
- Does the phone have a camera? You need to review every single image for identifiers before sharing them: does the image include a building, landmark, or scene that might indicate where to locate you?
- Does the phone allow you to block numbers?

Nottinghamshire Women's Aid, The Farr Centre, Chapel Walk, Westgate, Worksop, Notts s80 1LR
Telephone: 01909 533610 Email: enquiries@nottswa.org Web: nottswa.org

Nottinghamshire
Women's Aid
Survive & Thrive

INTERNET SAFETY

In order to stay safer you will need to change your online activity. 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.
Consistently applying a few simple rules, and staying vigilant, will do a lot to help you stay safer online.
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 where you live, exposing your friends list, blogging about what you're doing, leaving an 'away' message on your email saying where you're going: these may all expose your whereabouts. And it may not be you who exposes your whereabouts, someone else may accidently do it for you. Not only do you need to learn to hide information, but anyone who knows where you are, needs to learn to keep your privacy too.

If your abuser is someone you know - a spouse, ex, colleague, friend, etc. - they may have placed tracking or 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. 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, contacts, is being monitored until you've cleaned up these devices. If you aren't technically savvy, you may want to have a TRUSTED friend or family member help you, or use a pc repairer to do this for you.
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. Set the security software to automatically update, then your machines have the best protection possible. Do NOT leave your computer unprotected; this is like leaving your front door unlocked.
Make sure your wireless connection is password protected with a new, strong passwords.
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 new password to log on to your computers and phones so that no one but you can use them.

Email

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 in attempt to contact you.
Consider creating one or more new email accounts:
1. Create one email account for your most trusted contacts.
2. Another account for when you register on websites.
3. An email for financial accounts e.g. online banking or PayPal.
4. Lastly, create one account for contacts that you and the abuser both know – they may give your new email to the abuser.

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

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. Think carefully who you give it to and which sites you use it on. 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. An ex partner who knows your password or can guess your security passwords can access your online account.
Safe passwords don't have to be hard to create; they just have to be hard to guess. Use different passwords for each site so that, if one password is hacked then they won't be able to use the same password on other accounts. 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.

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. 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 careful when adding 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 will likely be able to see it.

Social sites

Social sites that allow you to share and get support are important tools for victims of abuse, but you have to be extra cautious when using social networks. If you or your friends are careless, it can lead the abuser to your new door/workplace or other location. Delete existing accounts! If you don't delete the account you may be tempted to check these accounts periodically, but if your abuser is aware of these accounts, they will continue to monitor them to glean information even if they are set to private. If you want to continue using an existing social networking site or forum, create a new account to avoid being tracked by an abuser.

Twitter and micro-blogging sites are designed to be public – in other words you can't make them private. Even if you are careful, what you say about your location, activities, or emotions, added together they may provide too much information to a determined abuser. That is why we suggest not using them.

Social networks like Facebook and Twitter have implemented location functionality that, if turned on, might show where you are whenever you post. Be sure that any location functionality in any online service you use is OFF this includes shutting off Bluetooth functions on mobile devices.
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 fictional information about location, gender etc.
- Don't put up a profile picture, an abuser may see your picture through a friends list.
- 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 very trusted people to join you. You should have a limited amount of friends.

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 restricted to only selected friends (who have their privacy restricted also), there is less risk in sharing it. However, if you say things that give your location, work or where you going out etc, that information could leak out to your abuser.

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, 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 to out or work, for example.