BEING WEB WISE

Information about our lives, including personal information, is increasingly ending up online. Many of us have concerns over the security and privacy of this sharing. Victims of domestic violence, sexual violence, and stalking have even more complex safety risks and concerns when their personal information ends up on the Internet.

How does my information get on the web?

To understand how information about you is getting collected, shared, and archived online, you need to first understand how information gets posted online. Information ends up on the Internet in one of two ways: either you post it or someone else posts it.

Information You Post

Below are some examples of ways you could be sharing personal information online.

- Posting updates on social media.
- Sharing your location by "checking in" or tagging photos through social-based location sites such as Facebook, Instagram, etc.
- Commenting on articles or blogs or writing reviews on shopping or consumer review sites such as Zomato or Trip Advisor.
- Creating wish lists or liking certain content through sites like Amazon, Etsy, or Pinterest.
- Sharing photographs or videos online.
- Interacting with other users through virtual worlds or online games.
- Inadvertently sharing personal information online, such as location data when uploading photos.

Even if the information you post may not seem to be identifying, it can reveal a lot about you. Posting a picture of your local school's mascot or a favorite restaurant might inadvertently reveal your location. Additionally, if the location setting on your phone is turned on for your camera application, uploading pictures taken with that camera may contain the exact location of where that picture was taken.

If you have joined any website where you create a profile page, make sure you know who can see that information. Depending on the site, that profile information may be available to other users (or the public). Typically, the default settings will allow anyone who visits that site (family members, potential employers, and stalkers) to see your personal information. Keep in mind that even if you are allowed to "lock down" your account through the privacy settings, some account or profile information may always be public (your user name, for example).

Safety Tips

- If you join sites where you create an account and a profile, check to see if you're allowed to change your privacy settings to minimise what others can see about you. These sites are meant to draw in as many people as possible and by default, your information may be available to anyone.
- Learn what the company does with the information you share with them by reading their privacy policy. Most companies will share your information with other business partners or even sell it to advertisers and marketers. Your personal information is valuable for many reasons, particularly for marketing and advertising companies.

Information Others Post About You

Anyone can post information about you, including your friends, family (including your children and current and former partners), employer, church, community groups, school, government, information brokers, and others. Information about you can come from different sources including:

- Court records
- Employer staff directories
- Web directories
- Newspapers
- Voting Registration Records
- Faith community/Work/School newsletters
- Social media sites

Public Records

Many courts now publish records online, often without providing notice or providing ways for citizens to request their records not be published to the web.

Voter registration information is considered public record and although not published online, can be viewed at any divisional office of the Australian Electoral Commission. Information available may include the registered voter's full name, associated residential address, and voter registration number. You can apply to be a "silent elector" if you feel that having your information on the electoral roll would put your (and/or your family's) safety at risk. If granted silent elector status, only your name would show up on the electoral roll.

Safety Tips

- When sharing information or interacting with any court or government agency, ask if any of your personal information will be posted online. Ask if there is an opt-out option and how you can opt out.
- Register to be a silent elector if you are concerned about your address being publically viewable.

Friends, Family and Colleagues

Most organisations and even many individuals have websites. If you have ever performed in an artistic event, been on a sports team, or spoken at a conference, your name, biography, and contact information may be on the host organisation's website. If you have been quoted by the media or highlighted by them for any reason, your information may be in other places on the web too. Community organisations may post newsletters online, including names of donors, volunteers, staff, board members, and even participants in fundraisers. Some Parent Teacher Associations (PTA) post minutes of their meetings and includes names of attendees. Even older information that wasn't originally online may still end up online since organisations and family members are scanning and posting old newsletters, pictures, or articles to the web.

Safety Tips

- Ask organisations that you are a part of if they have any publications or websites. If you are concerned about your privacy and safety, ask them not to publish your information.
- Be aware of what schools or employers may post online about you and your children.
- Ask friends and family members not to mention you, tag you, or post pictures or videos of you online.
- Be mindful when people are taking photos at events; if they post these photos to Facebook (and you don't have your privacy settings set up to meet your safety needs), Facebook may suggest they tag you based on the facial recognition software used.

How do I know what's already on the web?

Use a search engine like Google or Bing to search for yourself. "Search engines" (such as Google) index the web and create virtual card catalogs that link to the actual content. Search engines have existed since the web was developed and they are getting faster and smarter every day. Most search engines periodically "archive" or "cache" websites by saving copies of every webpage so that users can still access the content, even if the website is offline, has changed, or is otherwise unavailable. This means that any information ever published online could potentially be available forever (or as long as the Internet exists). Even if a website is changed to remove inaccurate or dangerous information, the old web content might still be indexed by a search engine.

Browse online directories for your information. Online phone directories such as http://www.reverseaustralia.com/, https://reversephones.com.au/ or http://www.reverseau.com/ include reverse phone look-up features where someone can search a phone number to find the name associated with that number and possibly the address or a map of the location. Even if your phone number is unlisted through your phone company, your address, phone number or a map to your house may be available through records obtained from marketing companies and other databases.

Browse websites where you think your information may be posted. Visit websites for groups and places that you're connected to: your job, faith community, sports teams, community and volunteer groups, etc.

Can I remove information that is inaccurate, false or that I don't like from the internet?

Search engines like Google and Yahoo typically aren't responsible for posting your personal information on the Internet. Often, they simply search to find all the websites that list your information. To fully remove your information, you will need to go to each of those individual sites and request that your information be removed.

Depending on the accuracy and sensitivity of the information, it may be best to leave it alone. Many survivors prefer to leave inaccurate information online to obscure the accurate information that is also available. If the information you find on the web is abusive or potentially dangerous, you can contact the website and ask them to remove the information. Most social media platforms will have reporting options where you can flag abusive content. Websites will remove content based on their terms of service and community guidelines.

Some sites might require additional information from you to prove that you are indeed the person the information is about. Only share what you're comfortable sharing. For example, if you're asking for a site to remove your phone number, but you must give them your physical address, driver's license number and a photograph to process the removal, that information may be more information than you're comfortable sharing.

Also, keep in mind that removing what an abusive person posted might alert to them that someone complained. Some perpetrators may respond by increasing their stalking, harassment, or abuse. Think through possible retaliation from the abuser in your safety strategies. If the information published about you on the web is extremely dangerous, inaccurate, or otherwise damaging, talk to a domestic or sexual violence counsellor for help and seek legal advice.

How do I prevent further information from being posted?

The best way to prevent more information from being posted online is to prevent the information from being collected in the first place. Although this is easier said than done, here are some tips to get you started:

- When a cashier asks for your phone number, you don't have to share it. In situations where you must provide a phone number, consider giving your work number instead of your home number.
- If you register for a super market/chemist discount card program, fill in very little information. Some stores have a "store card" that you can ask to use.
- Use a pen name when writing letters to the editor or posting online.
- Give donations anonymously.
- When possible, avoid paying with debit or credit cards.
- If you belong to organisations that have a website, ask that your name not be included in publications and ask that you not be "tagged" in photos that are posted online.
- When looking for jobs, don't post your resume on any of the career sites. Instead, search the web for available jobs and send resumes directly to those you're interested in.
- Ask friends not to blog about you, post things about you on social media platforms, or post photos or videos of you.
- Check all of your privacy and security settings on sites that you use, both on your computer and on your phone to ensure that you're not inadvertently sharing information.

In addition to preventing information from being posted online, you can try to monitor what does get posted. Set up a "Google Alert" that will email you any time it finds your name online.