

Keeping your personal information private

- If your personal information is requested, ask why. Why do they need, how will it be used, who has access to it, how long will it be kept on record, then decide if you need to provide it or not. It's okay to say no.
- Just because an agency or company asks for personal information, does not mean you are "required" to provide it. It is required only for IRS tax reporting purposes. Use alternate forms of verification or passwords.
- When applying for employment, you can write in "will be provided upon hire" in the SSN and date of birth block. Remember, many copies check social networking sites of potential employees. Make sure yours is marked private.
- Shred all personal and financial information, i.e. bills, bank statements, credit card offers, etc.
- Limit personal information in your wallet or purse. This includes decreasing the number of credit or debit cards you carry.
- Do not give out any personal information over the phone, especially your social security number, date of birth, etc.
- If you have on-line access, you may consider signing up for statements on-line to minimize theft from mail boxes.
- Get a post office box. It's just safer.
- Remove yourself from marketing lists to minimize the circulation of your information, junk mail and other offers www.dmachoice.org/MPS/mps_consumer_description.php
- Set up and use passwords on your credit cards, bank accounts and other accounts you access and monitor your account activity.
- Review your credit report annually—free. You can do so at www.annualcreditreport.com.
- Read the privacy policies. Many agencies can share your information so it is up to you to "opt-out" of that process.
- Many breaches of security are internal. Identity theft happens most often via family members and friends. Keep all personal documents in a secure place at home.

What is stalking?

Stalking is repeated unwanted behavior from an individual that is harassing, intimidating, and puts a reasonable person in fear. Stalking is most common in intimate partner relationships. Many times there will be an increase in stalking behavior upon leaving a controlling relationship. In fact, according to the Stalking Resource Center, 76% of intimate partner murder victims had been stalked by their intimate partner prior to their death.

Remember

Harassment = Annoying

Stalking = Scary.

Cyber Stalking in Washington State

Cyber stalking occurs when someone uses electronic communication to harass, intimidate, torment or embarrass another person. This can include things such as lewd, indecent, or inappropriate, pictures, comments, text messages, impersonation or posting of personal information through electronic means, website tampering, etc. Conversation does not have to occur between the two parties for this to be a chargeable criminal offense.

If you are being stalked or cyber stalked, take it seriously! Work with a domestic or sexual assault advocate to safety plan and document the stalking behavior.

Cyber Safety

Technology Safety Project

WASHINGTON STATE COALITION
WSCADV
AGAINST DOMESTIC VIOLENCE

1402 Third Avenue, STE
402
Seattle, WA 98101

Phone: 206-389-2515
Fax: 206-389-2520
TTY: 206-389-2900
www.wscadv.org

Cyber Safety

Internet & Computer Safety

- If you are researching resources to leave an abusive situation, use a “safer” computer. A computer your abuser does not have access to. This could be at a public library, trusted friend or family member’s home, work or computer lab.
- When setting up free email accounts or chat room profiles, never use your nick name, real name or personal information. Become someone else, it’s okay. Only fill out what is required on the form not simply asked. They don’t need your birthday, social security number, real address, phone, etc.
- Search for yourself on Google and Zabasearch.com. See what information comes up about you. Remember you can ask to be removed but most likely your information will pop up in other databases.
- Abusers often View internet history and cookie files to see where and what information you are accessing. If you erase these files, they will become suspicious. Use a safer computer.
- Purchase or download a firewall and keep all anti-virus software up to date to prevent malicious codes being downloaded on your computer. It is important to update your windows and software products to make sure you have the most current security patches and releases to protect your system.
- Read the privacy policies before giving information. They say, “We take your privacy seriously,” yet they still may retain the right to sell it to marketers.

Cell Phone Safety

- Do not store personal information, passwords or account numbers on your cell phone. If your phone is lost or stolen, think about what information someone can gain access too.
- Lock your key pad to prevent accidental dialing and malicious tampering. It only takes a few seconds for someone to access information on your phone or change the settings.
- If you have bluetooth make sure it is set to hidden or turned off so that you are not broadcasting your phone information to others around you. Through bluetooth your phone can be hijacked or sent a virus without you knowing it.
- Your phone is really a mini computer. Safeguard your information and “think B4 you click.”
- Text messages can be used as evidence if you are being stalked or harassed. Save them or forward them to an email account to be saved.
- Learn to text message. You may not be able to talk to get help but you can text a friend to call for help.
- The GPS system in your phone may be used to monitor your movements through friends and family plans. You may have to ditch or leave the phone behind if you are fleeing a dangerous situation. Domestic violence agencies can give you a free cell phone that can call 911.
- Don’t assume that emergency services can find you through your GPS chip. Sometimes maps are outdated and not accurate. Give your location information or landmarks.
- If you are the subscriber and account holder of your cell plan, consider signing up for web based services to review your charges on-line. Remember, anyone who knows your personal information can sign up as you and review your calls without your knowledge.
- If your phone number is not marked private, you can block your number on a one-time basis by dialing *67 then the number your are trying to reach. The caller id will say “unavailable or restricted.”

Email Safety

- Never let your computer program i.e. windows, save your passwords. Change your passwords often.
- Use different email addresses for shopping on-line, friends and work.
- Set up a separate account to communicate with someone that is harassing you. The messages become evidence if the person is charged with a crime.
- Never open an email from someone you don’t know. There could be a virus attached to it that can invade your computer such as spyware.
- When forwarding email, send it to yourself in the To: line, and use the BCC (Blind Carbon Copy) to forward the email to your friends and ask your friends to do the same to protect your email address.

Password Safety

- Use a combination of letters, numbers and symbols. The longer the password the harder it is to crack.
- Don’t use names, nicknames, birthdates, etc that someone who knows you well would be able to easily guess.
- Change your passwords often on all accounts, on-line and off, i.e. web accounts, banking, shopping, email, cell phone, etc.
- Never leave or store your passwords where they can be seen by others, like posted on your computer screen or on your desk.
- When an agency wants to use your social security number as a way to identify you, talk to them about creating a password or code. Many agencies grant your request if you just ask.