

Technology and Safety

Technology is always changing, which can both aid victims regarding safety AND provide new ways for abusers to stalk and harass their victims. This information can help you protect your privacy, for example by preventing the abuser from knowing who you call, who calls you, or the content of your private conversations. In addition, knowing how to use these same technologies can help you plan for your safety.

Computer, Internet and Email Safety

Computer technology can put your privacy and safety at risk. The hard drives on computers keep records of every action taken on the computer and Internet, and it is virtually impossible to completely erase these "foot prints." Even if your abuser is not an expert at computers, he may still be able to trace your computer usage, or can easily find someone that can. In this way, the abuser can steal your passwords and get other personal information.

If you think you may be monitored on your home computer, it may be safer for you to stop using that computer for research and contacts regarding your safety needs. Computers that are located in a public library, community technology center, Internet café, or at a trusted friend's house may be safer options if you wish to use email or browse the Internet.

Other precautions you can take include:

- Never share your email password(s). However, if you believe your abuser knows your password, you may want to consider whether changing it may cause more danger by arousing suspicion.
- Passwords should be difficult to figure out. Using a combination of letters and numbers can make your password more difficult to determine. Also, avoid using birth dates, street addresses, names, etc.
- Consider having more than one email account so that you have an alternative if your abuser forces you to close an account. Try to create an alternative email

account on a safer computer, such as the ones at the public library. When creating an account, leave out personal information such as your address or phone number, especially when using a web-based account such as Yahoo, Hotmail, GMail, etc.

- When you create your new email address, avoid using your name or a common nickname for you.
- Only share this email address with people you are sure will not share it with others.
- If you maintain online social networking site account, carefully screen the personal information that you post. Consider whether that information will give the abuser clues about where you are located or your daily routines. Also, talk with your family and friends who may have similar accounts and ask them to not post any information about you that may be harmful.
- If someone would like to send or forward you a message or reply to a message you sent, ask the individual to use the "bcc" function in the email the person is forwarding. Sometimes, people forward emails without deleting the original email addresses. This means you don't know or have control over how many people or who learns your new email, including your abuser or your abuser's family and friends. The "bcc" line is directly below the "cc" line. All email addresses put in the "bcc" line are invisible to anyone receiving the email. Also note that if you "reply all" to a "bcc", you are sending the email to all.

Computers can be a useful tool in accessing information about what you are going through and what you can do to seek help. However, some domestic violence websites are not legitimate and may give you misleading information. Your local domestic violence advocate can help sort out any information that may be confusing. Finally, emails from your abuser can provide excellent evidence in a court case. You may want to consider saving his emails, even if you don't have a case pending, so they are available if you ever need them.

Contact law enforcement or your district attorney's office about printing threatening emails from your abuser. They may want to send over someone to ensure proper evidence collection methods are used.

Protecting Your Personal Computer Accounts from "Spyware"

Never open emails from your abuser or an unknown person on your personal or work computer. If you have already opened such emails, or your abuser has had access to the computer or sent emails to that computer, you may already have "spyware" on your computer. This means a program has been installed to be hidden on your computer, and will monitor your computer activity and/or access your emails. While you can get anti-spyware software (like Spybot) and/or take your computer to a professional, the damage may already be done. To be confident about protecting your computer activities refer to the bullet points above explaining about computer precautions, second email account, etc. But most importantly, if you need to give someone confidential information that conversation should be done in person, over a land-line corded phone, or from a "safer" computer such as ones located in a public library.