SAFETY ON THE INTERNET

Please understand that **computer use can be monitored by an abuser,** and there are ways for an abuser to access your email and to find out what sites you have visited on the Internet. **It is impossible to completely clear all data related to your computer activity.** If you think you are being monitored, you probably are right. In order to stay safe you will need to change your online activity. The following suggestions cannot guarantee your safety, but they will help you learn how to take additional precautions, to better protect your anonymity, location, and identity.

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 are all things an abuser might be able to see. 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, MUST learn to keep the secret too.

Clean up your computers, mobile phones, and vehicles

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 he could have turned on the "parental controls" making you the 'child' account. Everything you do is reported to them. You don't have to be a computer 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. Assume everything you do or say online, including your passwords, calendar, email, contacts is being monitored until you've cleaned up these devices. If you feel you don't have the techy knowledge to do this, find a trusted friend or family member help you, or use the Geek squad or computer repair to do this for you.

If you do not have up-to-date security software installed, now is the time. If cost is an issue, there are excellent **FREE** alternatives you can use. Set the security software to automatically update, then your device will have the best protection possible. **DO NOT** leave your computer unprotected; this is like leaving your front door unlocked.

Now that your devices 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 the computer and phone so that no one but you can use them.

DO NOT SKIP these precautions. If your machine is forwarding all your information to your abuser, the safety tips outlined in the remainder of this guide CANNOT help you.

Create a new Email account – Stay anonymous

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:

1. Create one email account for your most trusted friends and contacts.
2. Another account for when you register on websites
3. An email for financial accounts, 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

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. You can have a Gmail account, a Yahoo Account and a AOL account. By importing all your accounts into one service, you can easily manage them all from one spot.

KEEP YOUR EMAIL PRIVATE

The two things to think about with email is; one, how strong is your password, and two, who you share your email address with. Think carefully who you give it to and which sites you use it on. You want to be able to contact, and be contacted by, those who support you, but avoid the abuser getting your email address.

Strong passwords are <u>critical</u>

If you lived with the abuser, or they had access to your computer at some point, you should assume that any passwords you have were compromised. Anyone who knows your password or can guess your security passwords can access your online account. If it is an email account he can read all your email or send out emails in an effort to sabotage your relationships with others. If it is an online shopping account he will see your current delivery address. An online banking account gives him access to your money.

It is vital to change all your passwords, NOW!!

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

Safe password safety rules:

Use a different password 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 (birth date, address, pets names, children's names) are easier to guess. Don't use 123456 or abcdef either.

How to create easy to remember secure passwords:

1. Use a long phrase that all runs together that is easy to remember. "It was a dark and stormy night!" Itwasadarkandstormynight. Or you can use the name of the website to make an individual password. Amazonandmyself.

2. Use words to create a standard pattern is an easy way to create passwords for every website you use. For example, you are creating a new password for Master Pass. Use the first 3 letters of the website,

username backwards. First 3 letters of website = Mas, + username backwards = joebloggs is sggolbeoj, you get Massggolbeoj.

3. Remove the vowels. Take a word or phrase and remove the vowels from it, eg. “eat the cheeseburger” becomes “tthchsbrgr”.

4. Use the keyboard to assist you with passwords. Hit the key to the left or the right of the word you want. For example: **evictims** using keys to the left becomes **wcuxruna.** Using above and to the left, **evictims** becomes **3f8d58jw.**

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 or pinned up on the wall!

Security question

Many sites ask you to answer a “password hint’ or ‘security question’ from a drop-down box. Unfortunately, many of the questions ask for answers that can be found in publicly-available sites such as your place of birth, a school you attended, or your mother’s maiden name. In cases of domestic 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. 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 the answer is correct, it verifies only that you can repeat the answer you gave before. For example: what is your mother’s maiden name? Purple Butterfly. Your first car? Purple Butterfly. The city you were born in? Purple Butterfly.