Website Safety Alerts

Tips for Advocacy Organizations

Why revise our safety alerts?

- Many advocacy organizations are developing websites to provide information to victims of domestic violence, sexual violence, and stalking.
- Victims are using the Internet to look for help, resources, and information.
- Technology has advanced to make it VERY easy for abusers to monitor all computer use, and thus, all computer activities of a victim.

How much is too much on the web?

From the moment we started safety planning with survivors, advocates have struggled to find the right balance of providing comprehensive and clear information to victims without inadvertently giving information to perpetrators that could increase the risk to victims. The ease of searching the entire World Wide Web has complicated this struggle even more.

If we publish detailed checklists of the hundreds of ways an abuser can monitor a victim's computer activity we could inadvertently provide information to abusers and stalkers that they can misuse to further harm victims.

If, instead, we provide clear, but brief information to victims on the Internet about their risk and encourage them to call us for more details, we may be able to balance our need to provide information to victims without increasing their risk.

What is the right amount of information for us to post on the Web?

1. **Victims need to see a brief safety alert as SOON as they arrive on ANY domestic violence, sexual violence, or stalking web page**, since they may be at increased risk for even viewing these websites.
2. **A brief alert should be at the top of every page** of a website since it is easy to enter a website on a sub-page (from a link or a search engine) and never see a website's homepage.
3. **On another page,** we can explain **SOME details about computer and Internet safety** WITHOUT giving too much information to perpetrators. We can more safely give victims additional details on the phone or in-person.
4. **Victims need to know the ease of monitoring and the impossibility of clearing the traces of computer activity** so they can make an informed decision about safety. It is important that we not make false promises of clearing "footprints".
5. **We can encourage victims to use a SAFER computer** at a library, a community center, or at a local advocacy program. This tip is especially important if a victim is researching options for an escape plan. Looking at bus tickets, shelter information, and housing classified ads on a home computer could increase risk.
6. **We can tell victims that it is possible to monitor all computer and Internet use and that it is impossible to delete all traces** WITHOUT going into detail about SpyWare and Keystroke logging and monitoring programs so as not to educate batterers regarding other tactics of abuse.

2 Step Approach

1. **Put a brief alert in a banner across the top of EVERY DV/SA web page** (not just on the home page) since it is very easy to come into a website from a sub-page, not the home page. If it is at the bottom of the page and a victim doesn't scroll down, she won't see the alert.
2. **Put a link in the banner to another web page** with more details about using a safer computer without trying to cover the hundreds of histories.

***If possible, define "safer computer"** in a pop up window, floating text, or on the safety web page. A victim might think a home computer is most private without realizing that a home computer might not be safe for her.

Sample alert for the top of every domestic violence web page: (this text can be posted)

Safety alert: computer use can be monitored and is impossible to completely clear. If you are in danger, please use a safer computer, call your local hotline, &/or call the National Domestic Violence Hotline at 1-800-799-SAFE. If you are at a safer computer, click **here** to read more.

Sample Safety Web Page (this text can be posted on your website)

Internet & Computer Safety

- Computers create records in hundreds of ways of everything you do on the computer and on the Internet.
- If you are in danger, please try to use a safer computer where someone abusive does not have direct access, or even remote (hacking) access.
- It might be safer to use a computer in a public library, at a community technology center (CTC) www.ctcnet.org (national directory), at a trusted friend's house, or at an Internet Café.

If you are in danger, please

- **Call 911,**
- **Call your local hotline, or**
- **Call the National Domestic Violence Hotline at:**

1-800-799-SAFE.

- If you think your activities are being monitored, you are probably right. Abusive people are often controlling and want to know your every move. You don't need to be a computer programmer or have special skills to monitor someone's computer activities – anyone can do it and there are many ways to monitor.
- Computers can provide a lot of information about what you look at on the Internet, the emails you send, and other activities. It is not possible to delete or clear all computer "footprints".
- If you think you may be monitored on your home computer, you might consider no home Internet use or "safer" Internet surfing. Example: If you are planning to flee to California, don't look at classified ads for jobs and apartments, or bus tickets for California on a home computer or any computer an abuser has physical or remote access to. Use a safer computer to research an escape plan.

Email is not a safe or confidential way to talk to someone about the danger or abuse in your life; please call us instead.

"Corded" phones are more private than cell phones or cordless phones.

Why not tell victims to "clear" and "delete" their trail?

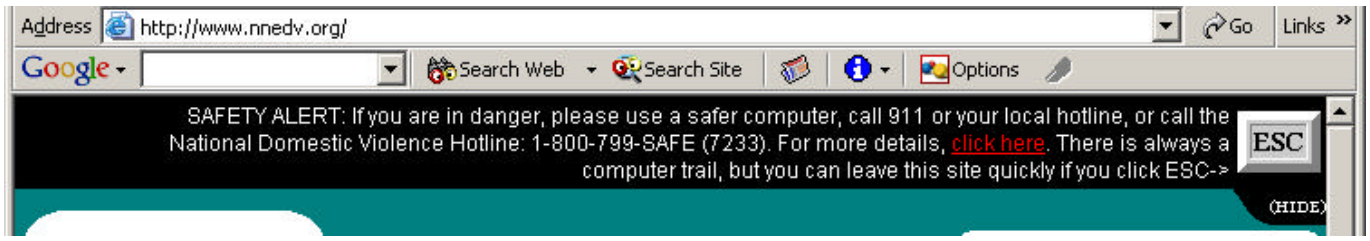
- We try to avoid using words such as "clear, remove, etc" since it is no longer possible to completely clear or remove your computer trail. If your organization insists on posting information about reducing your computer trail, then "reduce" is a better term than remove or clear. We also use the word "safer" computer, rather than "safe" since victims with tech-savvy abusers may have a hard time finding a computer that a batterer can't compromise.
- Telling victims to clear histories entirely could increase their risk and give a false sense of safety. It is not possible to clear ALL the traces on the computer. Also, if an abuser/stalker sees some empty histories or histories with nothing before the day they were cleared, the partner may become suspicious and escalate the control.
- We have stopped trying to explain how to clear history, cache, profiles, and cookies since we became aware of the hundreds of histories hidden in the computer and because SpyWare monitoring programs are being advertised EVERYWHERE. It is impossible to explain to women how to remove the hundreds of histories and trails – and especially impossible to cover every version of operating system, software version, etc.
- SpyWare resists all attempts to clear tracks; it records a victim's activities, then records her attempt at clearing her trail. SpyWare is impossible to detect without a police examination of her hard drive or the password from her abuser. Like computer viruses, there are hundreds of SpyWare/monitoring programs, some created by large software companies, others written by creative "hacker" types.

Why not give detailed explanation about SpyWare on your website?

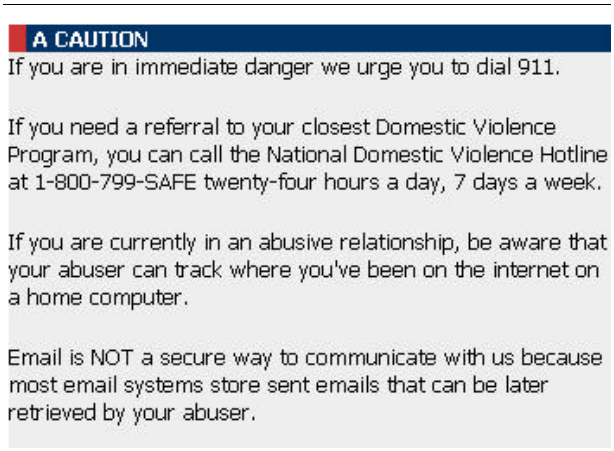
- For the abusers who only knew to check a victim's Internet History, too much information could put her in further danger. Telling a victim, in detail, about monitoring programs could help an abuser learn how to better monitor the victim.
- Posting clear, but brief information can provide critical information to victims without providing too much information to batterers. (Example: "People can see everything you have looked at on the web and done on your computer using many different ways. Please use a safer computer or call a hotline for more information.)
- Advocates can discuss computer monitoring as part of technology safety planning which advocates are encouraged to add to their current safety planning with victims.

Contact information for advocates and allies
(The project is not equipped for victim calls)
SafetyNet: the National Safe & Strategic Technology Project at the
National Network to End Domestic Violence
660 Pennsylvania Ave, SE, Suite 303, Washington, DC 20003
phone: 202-543-5566 SafetyNet@nnedv.org

Examples of different website safety alerts:



www.nnedv.org



www.wvcadv.org

www.kdva.org

www.tcadsv.org

www.kcsdv.org

www.gcadv.org

www.acadv.org

Sample Contact Forms (much safer than email addresses):