

Batterer's, Technology & Domestic Violence



Presented by
The Arkansas Coalition Against Domestic
Violence

Definition Cyber stalking & Harassing communications

- Threatening behavior
- Unwanted advances
- Directed at another
- Using the internet
- Computer
- Phone communications

Batterers' use of technology

- High tech eavesdropping
- E-mail tampering
- Monitoring home and internet activity
- Tracking the location of victims

High tech eavesdropping

- A Cell Phone = listening device.
- The phone never rings, but automatically answers.
- Some corded fax and answering machines also offer this feature.

High tech eaves dropping

- Use of a scanner to monitor communication.
- Victims should secure phone communication with a corded phone.
- Cordless phone may continue to broadcast even after it is hung up.

E-mail tampering

- Can intercept or re-direct email to their account.
- Can remotely check incoming email.
- Must also empty their "deleted email folder" in order to erase any record of the correspondence.

E-mail tampering

- For private correspondence set up a separate email account using a web-based email service such as Yahoo Mail or Hotmail.
- Note the web browser's History Log feature will show that the email site was visited, although it won't reveal the contents.

E-mail tampering

- Delete the History Log if this is a matter of concern.
- Almost all computer use, can be viewed by the abuser even if the history and temporary files are cleared.

Monitoring home and internet activity

- Use web cams and other hidden surveillance cameras to monitor.
- Web cameras are small devices about the size of ping-pong ball that can be installed almost anywhere.
- Images picked up by the camera's lens can be viewed via a web page.
- Victims are often unaware that these cameras exist.

Monitoring home and internet activity

- Internet browsers (i.e. Netscape and Explorer) keep several histories of recent sites visited on the web.
- Batterers can access these files to discover where they have been online.
- Spyware (i.e. Big Brother, WinGuardian, CyberPatrol, Spy Agent, and numerous others).

Monitoring home and internet activity

- These programs have the capacity to take pictures of the computer screen,
- Record a user's ID and passwords,
- Record both the sender and receiver's chat correspondence and incoming or outgoing mail.
- The software generates a report over the Internet to whomever is monitoring it.

Monitoring home and internet activity

- Newer email viruses allow remote control of the computer.
- Be very careful of opening any email attachments,.
- Run and update anti-virus software often.
- Other operating systems such as MacOS and Linux are much less vulnerable to back-door attacks.

Tracking the location of victims

- Batterers can use features like caller ID, last number call-return, and fax headers.
- Directory assistance can request an operator to look up an address that correlates to a phone number.
- Enter a special code or re-program fax to "block" number from being displayed.
- Free caller ID "line-blocking" can be placed on regular phone lines and fax lines.

Tracking the location of victims

- Careful of calling 1-800 type "call-me" numbers.
- Toll-free numbers report the phone number of the caller on the phone bill, even if Caller-ID blocking is established.
- Use pre-paid telephone cards.

Tracking the location of victims

- Global Positioning Software (GPS) technology.
- Batterers can install GPS in a car for less than \$300.
- The antenna is about one-inch by one-inch and requires a clear view of the sky.
- Victims may not realize what this antenna does or notice it at all.
- Once installed, the unit logs the location, time, and speed of vehicle at all times.
- There have already been reports of people installing GPS units to track their teenagers' and spouses' use of the family car.

Tracking the location of victims

- The cellular and PCS wireless industry has been mandated by the government to develop technologies that allow emergency personnel to pinpoint the location of a person using a phone, to call 911, for example.
- This has already been implemented in some areas.

How cyber stalkers target victims:

- Harassment in Chat rooms
- Message boards
- Discussion forums
- Threatening or Obscene E-mail
- Spamming (junk e-mail)
- Flaming (Verbal abuse)
- Sending electronic viruses
- Electronic identity theft
- Intercept or redirect e-mail

Cyber stalking & Offline stalking

Similarities

- Terrifying for victims
- Risk psychological trauma
- Risk physical harm and assault
- One can evolve to the other
- Excessive phone calls
- Vandalism
- Threatening and obscene mail
- Trespassing
- Both involve former intimates
- Most victims are female
- Both are motivated by the desire to control their victims

Cyber stalking & offline stalking Differences

- Predator & victim must be located in the same geographic area
- Technology makes it easier to harass/threaten a victim
- Technology lowers the barriers to harassment & threats

Types of Cyber stalkers

- Sexual harassment (most common)
- Love-Obsession (“breaking hearts”)
- Hate, revenge, vendettas (males & females)
- Ego & power trips (show off tech skills)

If you are a Victim of Cyber stalking

- Victims under 18 tell parents or another adult they trust.
- Victims should send the stalker a clear written warning that the contact is unwanted.
- Victims Never communicate with the stalker again after the warning.
- Victim may file a complaint with the stalker's Internet service provider, as well as with their own service provider.
- Save all e-mail, postings, or other communications in both electronic and hard-copy form.
- Save all of the header information from e-mails and newsgroup postings.
- Record the dates and times of any contact with the stalker.

If you are a Victim of Cyber stalking

- Start a log of each communication.
- Victims may file a police report or contact the prosecutor's office.
- Victims save copies of police reports and record.
- Victims may consider changing their e-mail address, Internet service provider, a home phone number, and should examine the possibility of using encryption software or privacy protection programs.
- Victims may learn how to use the filtering capabilities of email programs to block e-mails from certain addresses.
- Victims should contact online directory listings to request removal from their directory.
- No contact should ever be made with the stalker.
- Meeting a stalker in person can be very dangerous.

Potential Effects of Cyber stalking

Some of these effects may include:

- changes in sleeping and eating patterns
- nightmares
- hyper vigilance
- anxiety
- helplessness
- fear for safety
- shock and disbelief

E-mail Spoofing

- E-mail claiming to be from a system administrator requesting users to change passwords or suspending account
- E-mail claiming to be from a person in authority requesting users to send a copy of password or other sensitive information

Computer Privacy & Safety

- Hard drives record every action
- Impossible to erase “foot prints”
- Use computers in public places
- Never share passwords
- Passwords should be difficult to figure out
- Alternate account
- Never register personal info

Telephone Privacy & Safety

- Caller ID
- Anonymous call rejection service
- Call return
- Redial
- Call trace service
- Cordless/cellular phones can be heard by scanners and baby monitors
- Cordless phones can still be heard after hanging up (unplug for safety)

Advocates/Victim Service Providers

Should:

- Provide direct services and referrals to available resources that are specifically designed to assist victims of cyber stalking
- Train domestic violence and other victim service providers and advocates on Internet technology
- Name the behavior as cyber stalking and validate that a crime is occurring when working with individual victims
- Serve as catalysts in community efforts to form partnerships in the community
- Raise public awareness about the devastating impact on cyber stalking victims
- Inform public policy decision making

Mitigating Risks

- Domestic violence organizations must ensure that their practices do not further endanger people they serve or the staff members providing the services.
- Any response made with Internet communication, faxes or phones with Caller ID has the potential to endanger the safety of a victim if intercepted or read by someone other than the victim.
- Recognizing the safety implication involved with such a response is the first step to creating safer organizational practices.

Mitigating Risks

Safety and ethical issues involved with online service delivery and other innovative communication technologies include:

- a) violations of privacy;
- b) misunderstood communications;
- c) disinhibited communication and premature intimacy;
- d) rapid and wide spread of inaccurate information;
- e) cyber-addiction;
- f) misrepresentation of identity;
- g) unanticipated and burdensome obligations;
- h) lack of procedures and rules;
- i) online harassment and stalking; and
- j) a lack of knowledge about technology

Mitigating Risks

- These safety and ethical issues create liability issues for individual staff members, organizations, and perhaps technology developers.
- How should staff respond to an email message without possibly affecting a victim's safety?
- If a particular organization cannot help a victim, can staff forward email to another organization that may be better suited to meet the need?
- Can an organization be held liable if a victim is harmed as a result of receiving help online?
- Can the company that developed the covert monitoring software be held liable for the damage caused to a victim who was unaware that the program was emailing reports of her Internet activity to her partner?
- Finn (2001) reveals that no legal precedent has been established regarding these matters.

Mitigating Risks

Victims, advocates, and technology developers can undertake steps to initiate protective measures and therefore safer technology usage:

- Victims and organizations alike must first become aware of the implications involved with service delivery via innovative communication technology.
- Victims must recognize that their computers and wireless phones are not secure communication devices . Domestic violence organizations should develop criteria to evaluate web publishing content, especially with respect to assessment tools.
- Organizations should use disclaimers on web sites, create web forms instead of "mailto" codes for email messages, draft protocol regarding online response, encourage local, face-to-face support, and not use email as a long-term advocacy tool.

Mitigating Risks

- Technology developers should consider product testing with battered women's advocates, holding focus groups with battered women and their advocates, consulting an attorney regarding liability, and developing a public relations campaign about their technology developments that offer "safe features" for battered women.
- Organizations should also be conscious that technology can limit as well as liberate.
- The battered women's movement should develop guidelines and promising practices for online service delivery.

Cyber stalking Resources Online

- CyberAngels
- GetNetWise
- International Association of Computer Investigative Specialists
- National Center for Victims of Crime
- National Cybercrime Training Partnership
- Privacy Rights Clearinghouse
- Search Group, Inc.
- Working to Halt Online Abuse (WHOA)
