

Technology Tips in Cases of Domestic Violence & Freedom Balancing SAFETY, Sanity

Resources/Links

Safe Shelter of St. Vrain Valley (24 Hour Crisis Line)
303-772-4422 www.safeshelterofstvrain.org
LEVI (Longmont Ending Violence Initiative) 303-774-4534
www.LongmontDomesticViolence.org
Longmont Police Department 303-651-8555

NNEDV (National Network to End Domestic Violence)
SafetyNetProject.org www.nnedv.org

National Stalking Resource Center www.victimsofcrime.org
Privacy Rights Clearinghouse www.privacyrights.org

Google Voice – sets up online phone number that can
“blacklist” certain phone numbers www.google.com/voice
SpyBot- detects spyware – www.safer-networking.org

TrapCall – unmasks blocked/restricted numbers
www.trapcall.com



Basic Tips

Trust your instincts. If you suspect the abusive person knows too much, it is possible you are being electronically monitored.

Use unique passwords. Your passwords and PINs should be something the abusive person doesn't know or couldn't guess (avoid birthdays, pets names, etc). Set different passwords for your computer, phone & other devices, bank accounts, utilities, social media, wireless networks and email. Make a habit of changing your passwords frequently and don't share them with anyone.

Consider a home security system. Inexpensive home security systems with remote access video monitoring are becoming more available.

Conduct Regular Security “Audits.” Technology changes rapidly. Regularly verify you have the most restrictive security settings enabled on social media, computers and phones you use.

Be suspicious but not fearful. Don't answer emails, text messages, phone calls or instant messages from someone you don't know. Stay away from attachments you aren't expecting and screen all attempts to communicate with you. Don't be afraid of using technology; instead be smart and consistent.

A Word about Spyware/Malware



There are apps, programs and devices out there meant to track your electronic actions. Referred to as Spyware or Malware, these programs can be loaded on a phone or computer... sometimes through an email. It is hard to detect so if you suspect you're being electronically monitored, have your system checked. If your abuser knows information they shouldn't or your phone battery is draining rapidly be suspicious and have your devices checked.

If it isn't working

Sometimes, despite all the precautions put in place, the abuser breaks through. You can help document the contact by taking screenshots of unwanted/threatening text messages or emails, phone logs, or instant messaging conversations. Know that there is help available.

When to get more help

Abusers can be incredibly persistent and creative so it is important to know when you need more help. Below is a list of indicators that your situation is escalating or becoming more dangerous. Please contact the Longmont Police Department Domestic Violence Unit or the Safe Shelter of St. Vrain Valley for more comprehensive safety planning and intervention if you are experiencing any of the following:

- You are receiving multiple points of contact from the suspect (phone, email, texting, social media sites, showing up at work).
- You have taken steps to isolate yourself but the abuser is defeating your efforts to avoid contact
- The abuser has knowledge/information that they should not have.



While it is important to remain connected and maintain your support network when in an abusive relationship, being active on social media comes with certain drawbacks. Primarily disclosing your actions, whereabouts and plans. Below are some tips that will help limit your exposure on social media:

- Be wary of new friend requests.
- Ask your FB friends to block the abusive person so that connection is lost. Regularly check whether your friends are in compliance and unfriend them if they won't respect your wishes.
- Frequently check the security settings on your Facebook profile to make certain they are set to the most restrictive options.
- Pictures you post on Facebook may have a "geotag" (where they were taken) associated with them that can give information about your location.
- Social based location apps like Foursquare, Facebook Places and Google Latitude can be used to find you so stop "checking in" with these tools.
- Adjust your Twitter account settings. First, make your Twitter feeds private by selecting "protect my tweets," then be sure that automatic geotagging (location data tied to each tweet) is turned off. If geotagging was previously on, select "delete all locations data."
- Find friends the traditional way; Highlight, Blendr, Grindr and dating sites put you at risk of being found.

Phone Tips

Phones, particularly cell phones, serve as our lifeline. They house our email, contacts and calendar. SmartPhones provide access to the internet and a wealth of other information. Unfortunately all that access comes at a price...security. Below are some ideas to improve cell phone safety.

- Buy a pay-as-you-go phone like TracPhone for all contact with the abusive person. Only share the number with the abuser and you'll control when and if you want to communicate.
- Turn off "locations" on your phone and on all apps like Yelp, Urban spoon, Facebook, Skype, Groupon, etc.
- Put your phone in Airplane Mode so it's not sending data about your location.
- Minimize the use of cordless phones or baby monitors, they are easy to overhear.
- If you receive an unwanted call or one you suspect is from the abuser, hang up and dial *57 after the call. This is a call trace feature that alerts the phone company to track the call.
- Call your wireless phone provider to make sure there are no GPS tracking or family locator plans attached to your account. Ask for a security code on the account and specify users.
- Use a virtual number like [GoogleVoice](#) that transfers calls to your actual phone. GoogleVoice also allows you to blacklist certain phone numbers so you won't receive calls.
- If you get a new phone, manually enter contacts instead of transferring them.
- There are applications you can use to unmask calls coming from blocked or restricted numbers. One example is [TrapCall](#).
- There are applications you can install on your SmartPhone to easily record conversations you are having with the abusive person. GoogleVoice does this by hitting "4" during a phone call. Other apps to try are [CallRecording](#) or [TapeACall](#).

Don't assume your cell phone provider has a history of your phone records. Most companies only keep text messages for 72 hours. Get in the habit of saving all call logs, texts and other attempts to contact you made by the abuser.



Much like phones, computers make our lives much easier but also can be misused by abusers. Below are some ideas to increase your computer's security.

- Password protect your wireless network and only work on locked/secure wireless networks.
- In some cases (especially if abuser has access to your computer), you may want to think about using a web browser like [Tor](#) that scrambles your IP address.
- Create a new email account for all correspondence with the abuser.
- If you are using a free email service (Yahoo!, Gmail, etc), use a creative email address instead of anything that contains all or part of your name.
- Turn off your BlueTooth connection and completely shut down your computer after use.
- Create a [GoogleAlert](#) about yourself. This service scans the internet for items that match your name on a daily basis and sends you an email with the results. Simply go to [google.com/alerts](#) and enter your name and other information to create an alert.

"It has become appallingly obvious that our technology has exceeded our humanity" -Albert Einstein