TECHNOLOGY ISSUES FOR VICTIMS AND VICTIM SERVICE PROVIDERS

PRESENTED BY:

LUCY CARRILLO
OBJECTIVES

*Upon completion of this module the participant will be able to:*

- Better understand the overall technology issues that may affect victim safety.
- Better understand the technology issues that should be taken into account in safety planning with victims.
- Better understand the technology issues that should be covered by the practices, protocols and procedures of victim services agencies and advocates in their work with victims.
Why are we talking about this?

- Advocates and victims use technology on a daily basis.
- Along with the benefits, the use of technology has many risks that may impact victim safety and advocate confidentiality.
- Many technologies can be easily used in the perpetrator surveillance behaviors common in domestic & sexual violence and stalking.

Objectives

- An overview of the relevant technology issues.
- Technology issues to consider in safety planning with victims.
- Technology issues to consider for agency practices and protocols.
- A better overall understanding of these technology issues.
**Telephones – Cordless Phones**

- Cordless phones are susceptible to having calls intercepted by scanners, ham radios and to “crosstalk” on devices such as baby monitors and other cordless phones up to a mile away (1/4 mile is a “normal” range).

- If you switch during your call to a corded phone and hang up the cordless phone, the cordless phone’s base continues to transmit the call unless you unplug the base/transmitter.

**Cordless Phones - continued**

- Even new cordless phones (i.e. 2.4 GHz or 5.8 GHz phones with “spread spectrum” capability that jump frequencies during a call) are susceptible to interception by high end scanners.

**Cordless Phones – Recommendations**

- Do not use cordless phones unless really necessary.

- Advocates should inform victims of the possible risks of using cordless phones.

- If it is necessary to use a cordless phone, avoid mentioning any details and identifying information that would compromise victim safety or confidentiality.
**Telephones – Corded Phones**

- Corded phones may be tapped from inside or outside the building. The tap may be hooked directly to a tape recorder or it may transmit the call to a remote recording device/receiver.
- Caller ID boxes may be installed without the victim’s knowledge (i.e. in the basement).
- Recommendation: Use caution where there is a known safety risk. Avoid mentioning identifying and planning details.

**Telephones – Cell Phones**

- Calls can be intercepted by scanners, other cell & cordless phones and devices such as baby monitors.
- Newer digital cell phones (2.4 GHz and up) are much more secure but they can switch to the easily intercepted analog mode depending on antennae coverage (especially in rural areas).

**Cell Phones - continued**

- Some cell phones can be programmed to answer calls automatically. If the ring is also silenced, the abuser can “plant” the phone, call it, and hear everything going on in the room. The cell phone becomes a “bug” the abuser can call at will.
- “Spy Phone” cells can monitor both sides of all calls and even all conversation when the phone is hung up. Still very expensive.
Spy Phones - Hardware

Nokia 3310 Spy Phone

- You can use this Nokia 3310 Spy Bug Phone as a regular mobile to make and receive calls, send texts and so on. The Spy Mode feature enables you to leave the Spy Phone unattended and then dial into it from any phone anywhere in the world to listen in to what is going on around it. The audio quality is superb and the phone will not light up, make a sound or indeed give any other sign of life. Onlookers can even handle the phone and push buttons...the phone will appear totally dead. $1,799

Spy Phones - Software

- Call Magic Features: (Ground breaking technology
- Silently Answer Incoming Call from a pre-defined number.
- Runs in “Real Background” mode
- Automatically starts when is switched on

Cell Phones - continued

- Enhanced 911 requires cell phones to have GPS capability. This is great if emergency dispatch needs to pinpoint your distress call.
- However, this capability can be used by perpetrators to track and locate victims. Subscription services are available that will allow someone to go online and pinpoint the exact real-time location along of a cell phone, sometimes even when it is turned off. Some of these services will also provide a travel “history” of all movements.
Forget those piddly wiretaps. The next frontier in warrant-free surveillance is upon us, and it's open to everyone. A UK service called World Tracker apparently uses cell tower data (or GPS, when available) to track the location of just about any GSM cellphone. Just enter the number you want to track into the service's handy Google Maps-based interface, and you'll be able to zoom in on the device's location, with accuracy somewhere between 50 and 500 meters.

World Tracker turns anyone into a cellphone spy

Cell Phones - Recommendations

- Use newer, digital cell phones (2.4 GHz +) and if possible set so GPS works only with 911 calls.
- Especially avoid using cell phones anywhere you are known to frequent (i.e. home, office).
- Use caution where there is a known safety risk. Avoid mentioning identifying and planning details.
- When fleeing/leaving, leave the cell phone behind. Cell phone donation programs – no plan required to dial 911.
Telephones – VOIP

- Voice Over Internet Protocol is broadband Internet based phone service (i.e. Vonage).
- VOIP phones do not always connect to 911. Victims using VOIP should register their primary address with E-911.
- You can’t tell where someone is calling from.
- Easily tapped as it is unencrypted.

Telephones – VOIP

- VOIP software can be configured to unblock the “Calling Party Number” with each call.
- Call logs, voicemail, etc. are on the computer.
- Doesn’t work well with many alarm systems.

Telephones – Anonymizers

- Spoofing via spoof cards or websites allows victims or perpetrators to hide their location and identity – even disguise their voice.
- They can display a different number than the one they are calling from and some offer a call recording option.
- Websites such as Camophone.com utilize VOIP and keep no records of callers or calls.
- Also see Spoofcard.com, Telespoof.com, itellas.com.
SpoofCard calling cards offers you the ability to change what someone sees on their caller ID display when they receive a phone call. Key Benefits: Make calls truly private, Ability to record calls, Change your voice, Fun and inexpensive, Easy to use and fast to set up! Instant Access!

SPOOF/CARD FEATURES:
- Caller ID Spoofing
- Voice Changer
- Call Recording
- Web Control Panel

No computer needed! Simply dial the toll free number from the calling card you purchase.

1. Enter your pin number.
2. Enter any Caller ID number you wish to display.
3. Enter Destination number.
4. Choose the voice you would like to use.
5. Your call is connected using the specified Caller ID number.

As an added bonus, we offer you the option to record your conversation for FREE which you can later retrieve by logging-in to your control panel or calling our 800 number from anywhere.

In addition, we also offer the ability to change your voice to sound like a man, a woman or yourself for FREE.

Telephones – General

- All agency phone and fax lines and any other phone lines used by advocates should have their lines blocked for Caller ID and be TESTED REGULARLY to ensure it is in place.

- Safety planning and agency policies should include education and planning in regards to Caller ID and phone use in general (if or when to call, *69, redial, etc.).

- Verify the identity of the caller before discussing anything of substance.

- Advise clients that most phone companies provide the capability for online billing records for phones, calling cards, pre-paid cell phones, etc. The abuser may have access to these records or pay a service to get them.

- Stalkers may access voicemail and answering machine messages remotely.

- Stalkers may use reverse lookup to find who a phone number belongs to (i.e. AnyWho.com).
Global Positioning Systems (GPS)

- GPS devices map the position of the device to within a few square yards.
- Because they work off satellites, they perform even in the most remote areas.
- The devices can be very small and inexpensive. Necklaces, watches, bracelets, etc. are built containing GPS transponders to track the location of pets, children, the memory impaired, etc.
- New services that map the location of “friends” are growing in popularity (i.e. MapQuest Find Me or Follow Us).

GPS Locator Sample

Our SlimTRAK GPS ULTRA Tracker makes all others obsolete! Google & Windows Live Satellite Mapping with Birds Eye View is available!

- Weighing in at only 7.2 ounces, the all new SlimTRAK real time tracking system makes all others obsolete for more complicated wiring or GPS antenna mounting. Due to new state-of-the-art “high sensitivity antenna” technology, the very small SlimTRAK tracker is completely self contained, including 4 standard “AA” batteries that power the unit for a full 3 months. Of course, if you prefer a permanent installation, connection assembly with battery back up is also available.

- INSTALLS IN SECONDS: Once activated, SlimTRAK can be installed just about anywhere in the vehicle, under seat, in glove box, or any other convenient location. Not recommended for use in a trunk. For covert applications, our custom fitted waterproof magnetic case allows for quick installation under the vehicle or under hood. Unit can easily be moved from one vehicle to another. Also great for protecting heavy equipment, boats, industrial equipment and dozens of other items.

- EXTREMELY EASY TO USE: No rocket scientist need here! Unit operates using GPS and GSM communication technologies. To track your vehicle, simply access the SlimTRAK website from any internet active computer, type in your password, and a detailed map with tracking information appears. It includes time, speed of vehicle, street address of vehicle and last stop. Updates as little as every 2 minutes if desired. Toll free customer support assures that all your questions be answered promptly.
Satellite View: When you click on one of the dots, location data is displayed.

GPS - Recommendation

- If a victim notices their abuser showing up in places that they can't understand how the abuser knew they were there, GPS tracking may be occurring. Try to locate a GPS device and/or get a new cell phone.

- If a GPS device is suspected or located as "planted" on the victim, law enforcement may be able to use that to trap the abuser.
Fax - Recommendations

- Use a blank fax header without the phone number of the fax machine or the agency name.
- Ensure that the fax line is blocked from Caller ID.
- Verify identity of sender.
- Do not retain faxes that may compromise confidentiality and security.

TTY - Recommendations

- Verify identity of caller as abuser could be posing as the relay operator.
- Clear call history and suggest the victim also do so.
- Destroy call printout.

Personal Computers – Internet Use

- Any Internet use leaves numerous traces on the computer that can easily reveal what sites were visited. Even if you clear the browser history file & locator bar and delete all the “cookies”, there are still traces of the Internet sites buried in various places (i.e. cache files). These trace “footprints” of Internet use are fairly easy to find and virtually impossible to completely eliminate.
- WiFi and Bluetooth connections can be accessed within their range to steal data, tap into communications or “hijacked” and run by the abuser.
Personal Computers – Internet Use Recommendations

- Victims should be advised not use a computer that their abuser has access to for any Internet use related to their victimization. Use a friend’s or one from a library, school, etc.
- Victim service agencies should post highly visible warnings on every page of their websites and include directions, or links to directions, on how to remove the most obvious “footprints”.

Personal Computers – E-mail & IM

- E-mail and Instant Messaging are not confidential methods of correspondence. They are subject to interception, impersonation and hacking.
- Victims should shut off their Bluetooth functionality unless they are using it and/or set the device (i.e. headset) to “hidden” to make it much more difficult to hack into.
- Victims should not use a computer their abuser has access to for e-mail or IMing.
- Victims should use free, web based e-mail accounts set up with false names, etc.

Personal Computers – E-mail and IM Recommendations

- Victims should not have e-mail user names and passwords with ties to themselves. Change passwords often.
- All should verify the identity of senders. Do not open attachments from unknown sources.
- Do not retain email electronically or on paper that would threaten safety or confidentiality.
- Ensure that victims are aware that abusers may impersonate them via emails or IM’s to friends, relatives, employers, etc.
**Personal Computers – E-mail and IM Recommendations**

- All should verify the identity of senders. Do not open attachments from unknown sources.
- Do not retain email electronically or on paper that would threaten safety or confidentiality.

**Personal Computers – E-mail Recommendations - continued**

- Never use victim/client names and other identifying information in e-mail.
- E-mail and IM policies should be included in your agency policies.
- Agencies should not have victim specific information on computers that are directly or indirectly (i.e. via LAN) connected to the Internet.

**Personal Computers - Spyware**

- Spyware can be remotely installed on your computer without your knowledge (i.e. from opening an e-mailed greeting card that appears to be from a friend).
- Spyware can send all of your computer use including e-mail, chat, Internet use, keystrokes and screen shots to the installer.
- Spyware is transparent to the user.
- Spyware protection and/or detection software does not always work.
**SpyWare Sample**

![Spyware Sample Image]

**Keystroke Logging Hardware**

![Keystroke Logging Hardware Image]

**Personal Computers – Spyware Recommendations**

- Victims should be advised not use a computer that their abuser knows about for any Internet use related to their victimization. This includes not using the computers of friends and family known to the abuser. Use one from a library, school, etc. and use different ones when possible.

- Use virus protection software and other forms of “firewalls” but don’t depend on them to be always effective.
Computer Databases

- A name and SSN is all that is needed to get a victim’s credit report showing the most recent employment, address, bank accounts, etc.
- Governmental agencies continue to make more “public information” available online (i.e. court records, motor vehicles, tax data, voter registrations, etc.
- Retail chain stores increasingly database customer information (dept. stores, grocery, video rental, oil change, etc.).

Computer Databases - continued

- To the extent that some of this information is not available to the general public, for a fee, there’s a Internet based detective agency or service that will get it for the abuser (i.e. the Amy Boyer case).
- Sometimes simple, easy to use, and inexpensive “hacker” software can be used to access non-public database information.

Computer Databases - Recommendations

- Victims not wanting to be “found” should enroll in their State’s Address Confidentiality Program.
- Do not give out phone numbers or have them printed on personal checks.
- Google the victim’s name to see what online information is currently available.
Computer Databases - Recommendations

- Also check www.zabasearch.com.
- Victim specific information should not be stored on a computer that is hooked to the Internet.

Computer Database Recommendations (continued)

- Providers must guard against “social engineering” hacking.
- Victims should not use stores that database your name and address or use customer discount cards. These names and addresses can be hacked or sold.
- Victims in hiding might consider feeding disinformation to public databases to promote the appearance that they are living elsewhere.

Cameras

- There are a large number of “spy cams” on the market. Sometimes they are unobtrusive “nanny cams” or security cameras.
- Sometimes they are hidden in lamps, clock radios, smoke detectors, air purifiers, clocks, speakers, sprinkler heads, etc.
- Generally they use a wireless transmitter to broadcast video to a receiver which is often attached to a VCR or computer for recording. Sometimes they are activated by motion detectors.
Abusers are often very clever and willing to put large amounts of effort into their surveillance activities. Many of these technology-based methods are easy and inexpensive to implement.

If you suspect a victim is being watched somehow, try to determine what is the most likely method being used. Once identified, it can be used to protect the victim and sometimes can be used against the abuser.
**General Recommendations - continued**

- Avoid using computers, telephones, faxes, etc. for any information specific to identity, safety planning, etc.
- Do not rely on “high tech” phones, firewalls, etc. to make your electronic communication 100% secure.

**Closing Tip**

- DV victims often have trouble believing something other than their partner really loves them but has anger management issues.
- Advocates sometimes find it useful to have victims look at the abusing partner’s behavior from the stalking perspective. This can help a victim realize that some of their abuser’s behaviors are cold, calculating and manipulative, not done in the heat of anger.

**Resources**

- National Network to End Domestic Violence
  [www.nnedv.org](http://www.nnedv.org)
- Stalking Resource Center (National Center for Victims of Crime)
  [www.ncvc.org/src](http://www.ncvc.org/src)
- Allison.Vachon@doj.nh.gov, 603-271-1208