Communicating with Deaf Victims:
Supporting Safety, Increasing Our Responsiveness Through Technology

KERI DARLING
Why Tech Safety Planning

• Technology used daily by survivors (pagers, searching for resources and safety planning)
• Abusers and stalkers misusing technology to further control, monitor and harm survivors
• Information being published about people (public records) in databases on the internet (court records, property tax appraisals & voter records)
• Agency technology use – can impact confidentiality of survivors
Your Relationship with Technology?

- Not on Speaking Terms
- Cordial Working Relationship
- Very Intimate
Equipment and Services Used

• TTY
• Cell phone
• Email
• Internet
• Videophone
• VRS
• Relay services – TTY, IP, Online, VRS, Captel
TTY (Teletypewriter)
TDD: Telecommunications Device for the Deaf
Group Activity

• One group talk about the safety ideas

• One group talk about the risks

—Assign someone to report to whole group
TTY RISKS?

- Verbatim conversations printed and/or stored in memory
- Computer-based history nearly impossible to erase
- Impersonation is easy
- Access to 911

• Legal:
  - Misuse may violate eavesdropping, stalking (continued), impersonation laws.
  - Some types of misuse may also constitute a monitoring communications crime or an unlawful use of the TTY service.

  – What else?
TTY RISKS? (2)

- You can’t hear what is happening in the background or who else might be present.
- A TTY display is visible and can be read from several feet away.
- Most TTY’s have a memory. Your call will be preserved in the machine and could be replayed by anyone with access to the TTY.
- Most TTY’s have a printer that records your conversations.
- Shelter screenings can take a long time.
- Many Deaf people are not fluent in English or comfortable with complex English-based TTY conversations.
- TTY users use a wide variety of abbreviations which can be confusing for people who rarely use the TTY.
TTY SAFETY

– “read back” memory may need to be erased on both survivor’s and program’s machines
– Identify code words or phrases to avoid impersonation
– DO NOT print out and save conversations with survivor unless you have explicit permission
– Survivors should have copies made of print-outs if using for evidence, as ink may fade quickly
TTY SAFETY (2)

Know TTY, Relay, & Interpreter resources

Safety plan about using these 3rd parties

Talk to victim about potential TTY impersonation & develop a system for identifying victim

Safety plan around TTY machines, history settings

Do NOT save printed conversations
Cell phone- Droid, Iphone, blackberry .........
Group Activity (2)

• One group talk about the safety ideas
• One group talk about the risks

—Assign someone to report to whole group
PHONE RISKS

• Messages can be falsified or spoofed from the carrier’s website or services like Fake My Text available at http://www.fakemytext.com.

• You don’t know who is sending messages?

• Call history (all out-bound and in-bound calls) can be monitored directly on device or online records; online billing records show same info as paper records.
**PHONE SAFETY**

- When sending email or text messages, you never know who may have gained access to the hand-held device, or who will gain access in the future.
- Suggest that the person may want to delete your messages or numbers as soon as possible. **It can be difficult to delete everything, especially sent messages.**
- Ask the person what types of information are safe to send, and whether and how it will be safe for her to receive your messages or pages.
- Suggest the person put a “lock” on her device to prevent anyone from using it without her password.
PHONE BENEFITS

• When law enforcement presents carriers with a valid court order, the carrier MIGHT be able to search backup media to retrieve messages that were "deleted" from the device and their servers up to a year earlier.

• Law enforcement often take photographs or video of the phone & text message content for evidence.
PHONE BENEFITS (2)

• Survivors use for convenience and safety. May work in an emergency when voice service doesn’t. Can quickly communicate to large number of people.

• Legal: Nearly all 50 states now have laws that explicitly include electronic communication in their stalking or harassment laws.

• Customers can add a password to their account to prevent someone from accessing their account illegitimately.
Best Practices

• Encourage survivors to become familiar with all features of phone – including bluetooth.

• If using cell phones to respond to hotline calls in an area where you still have analog coverage, use sparingly & avoid identifying details.

• Ask if the abuser/perpetrator/stalker works for phone company or law enforcement.

• Phone donation programs – they are wonderful! The Wireless Foundation and Verizon Wireless donate working cell phones to programs for victims.
Computers/Emails
Group Activity (3)

- One group talk about the safety ideas
- One group talk about the risks

– Assign someone to report to whole group
EMAIL RISKS

• You can’t use the person’s voice to identify her, or to determine if you are communicating with a man or a woman.
• You can’t hear what is happening in the background or who else might be present.
• A computer display is visible and can be read from several feet away.
• Computers store emails and instant messages, which sometimes can be accessed even after they have been “deleted”.
EMAIL RISKS (2)

• Many Deaf people are not fluent in English or comfortable with complex English-based written conversations.

• Some Deaf people use a wide variety of written abbreviations which can be confusing for people unfamiliar with them.

• 911 calls placed from digital or computer-based phone systems will not automatically provide your location unless you have registered your address with your phone service provider.

• Power OR internet outages disrupt digital phone/communication services.
EMAIL RISKS (3)

- Emails are as public as postcards.
- Impossible to erase history.
- “Window Washers” have severe limitations.
- Firewalls, anti-virus programs, SpyWare detectors offer very limited identification of SpyWare.
- Wireless networks are not always secure.
EMAIL SAFETY

• Ask: “Is this a private email address? Does your [partner or the perpetrator] know about it?” Provide information about how to get a private and free email address and keep it confidential by accessing it only from safe computers. Contact the NW office for assistance.

• Ask: “Is he/she good with computers?” “Do you think he/she might be using spyware* to spy on your computer use?” If so, it may not be safe to use a computer the perpetrator might be able to access. The perpetrator might be able to retrieve even deleted messages and track the caller’s internet usage.
EMAIL SAFETY (2)

• Spyware is computer software that is installed on a personal computer to intercept, monitor or take partial control over the user's interaction with the computer, without the user's informed consent. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, and can also interfere with user control of the computer in other ways.
• Suggest that the person may want to delete your emails, instant messages or numbers and “Empty Trash” as soon as possible. This is especially important if the discussion has included confidential information like where and when she will meet you or the location of your office or support group.

• Establish a code name or word with the person at the earliest opportunity; use it to identify the person each time she contacts you, and before any confidential information is transmitted.
EMAIL SAFETY (4)

• Offer opportunities for face-to-face meetings with interpreters present.
• If the person is fleeing, suggest that she take the computer if possible.
• Suggest that she maintain a land phone line if possible, or explore other options for calling 911 in an emergency.
EMAIL SAFETY (5)

• Have more than one email address – work, home, anonymous, online ordering, etc.

• Using a safer computer, create new email/IM accounts the abuser doesn’t know about. Only check these accounts from that safer computer. Use new secret passwords – no birth dates. Don’t use your name as part of your email address.

• Ask friends/family not to share your new email address or screenname. Remind them to use BCC when emailing large groups so that your contact info remains private.

• Consider having a separate account for emails/IMs regarding custody & visitation.

• Use letters, numbers, and characters in your password, and change it frequently.
EMAIL SAFETY (6)

✓ Remember, anyone who emails might be surviving abuse...even if the person does not disclose they are a victim.

✓ Never send client names or identifying information in email

✓ Use web forms instead of “mailto” email addresses on Organizational websites. Include features that promote “informed consent” in your web form.
WIFI SAFETY

– Secure your session: Use a firewall and VPN tunnel to secure your data after logging into the access point
– Know your service providers security policies
– Use a wireless broadband card
– Change your home or office default router such as Linksys, or Netgear to a different name
– Disable automatic windows connection feature
BEST PRACTICE EMAIL

• Have organizational policies about how to most safely respond to email, instant messages, and text messages from victims.

• Remember, anyone who contacts you might be surviving abuse, even if the person does not disclose they are a victim.

• Use web forms instead of “mailto” email addresses on your websites. Include features that promote “informed consent” in your web form.

• If you reply, ALWAYS erase the original message to reduce the risk of sending survivor details to . . .
VIDEOPHONE
Group Activity (4)

• One group talk about the safety ideas

• One group talk about the risks

—Assign someone to report to whole group
VIDEOPHONE RISKS

• If your program has a video phone: Make sure it is programmed to show NO NAME to people receiving VP to VP calls.

• When using a relay service you can’t use the person’s voice/image to identify her, or to determine if you are talking to a man or a woman.

• You can’t hear/see what is happening out of the range of vision of the Video Phone or who else might be present.
Most Video Phones have a memory. Your number will be preserved in the machine and could be seen by anyone with access to the Video Phone.

A Video Phone display is visible and can be seen from several feet away.
VIDEOPHONE RISKS (3)

– Remote
– Cords – power/AV, etc.
– Online/Software account (Purple, ZVRS, NTouch, etc.)
– Record conversation (Z-150, VCR, camcorder etc.)
– Calls stay in data base or on VP device
VIDEOPHONE SAFETY

• Ask the person if she is in a private and safe place.
• Ask the person to erase her Video Phone memory at the end of your call.
• Establish a code name or word with the person at the earliest opportunity; use it to identify the caller each time she calls, and before any confidential information is transmitted.
• Offer opportunities for face-to-face meetings with interpreters present.
VIDEOPHONE SAFETY (2)

• If the person is fleeing, suggest she take the Video Phone with her if possible.

• Suggest that she maintain a land phone line if possible, or explore other options for calling 911 in an emergency. Video Phones are dependent on internet connections. A land line can increase options for getting help.
VIDEOPHONE SAFETY (3)

– Only VP when no one else is around/home
– If main VP is shared, make sure to delete numbers (dialed, received, missed, etc.)
– Make appt to VP (when safe), confirm appt
– Discuss back up options in case need to use alternative VP method
– If PO in place and abuser calls, can take a picture to prove violation
  • Can change settings for call alert
  • Can call VP Provider to block that number
  • Can call VP Provider to change survivor’s VP number
RELAY SERVICES

Online Relay

Sprint
Together with NEXTEL

http://www.sprintip.com
Sprint.com  |  Personal  |  Business  |  About Us  |  Contact Us

Sprint IP Relay

Product Information
- Software Compatibility
- Product Descriptions
- Need for VRS?
- Need help?

Announcements
- Sprint with VRS
- Relay order calls with VRS

Customer Care
- Take the survey

Preferred Language
- English
- Spanish

Sprint IP Relay is designed and engineered to meet and exceed the relay needs of deaf and hard-of-hearing individuals. Sprint IP Relay customers can order their relay service online or by calling 1-866-849-1529.

Your Privacy Rights: Acceptable Use Policy and Video Agreement: Copyright Notice: Find A Store: Contact Us

© 2005 Sprint Nextel. All rights reserved.

VRS
Video Relay Service
Group Activity (5)

- One group talk about the safety ideas
- One group talk about the risks

- Assign someone to report to whole group
RELAY RISKS

• You can’t use a person’s voice to identify the person.
• Depending on their service provider, some users may not be able to call 911 through VRS.
• It is more difficult to access a record of a conversation than with TTY.
RELAY RISKS (2)

- Harassment thru IP Relay
  - “This is operator 5243 we have a message. You’re a heartless, sick, nerdy b@$#$%. Die and go to hell. End of message. Thank you IP relay…

- Always a third party involved
- Conversations may be monitored through spyware or histories
RELAY SAFETY

– If want VP number blocked can ask the interpreter to block it before dialing
– If PO in place, and abuser calls VP, can take a picture
– Against FCC to have interpreter tell hearing person what individual looks like (including gender)
– Caller ID – phone number will show when calling thru VRS
NEXT STEPS....

• Create Action Plans – how can you increase safe and strategic use of technology in your work?

• Train colleagues: staff, volunteers, & board

• Increase technology skill in your organization: on your board, staff, volunteers. Nurture technology passion.
STEP 1

Educate yourself: Learn how assistive technologies benefit individuals who are Deaf or have disabilities.
STEP 2

- Discuss privacy and safety risks with survivors, including how perpetrators can misuse assistive technologies.
STEP 3

• Conduct accessibility assessments of your program. Identify barriers that keep victims from fully accessing services. Commit to immediate steps, longer term activities, and a strategic plan with the goal of eliminating barriers.
STEP 4

• Support the rights of each survivor to access the assistive technology that best meets their needs and preferences.
STEP 5

• Collaborate with disability rights organizations, Deaf schools, Deaf advocates, Independent Living Centers, Assistive Technology agencies, and other groups to ensure you can meet the needs of people who are Deaf.
CHECKLIST

• Can/ will you use text if that is what victim prefers?
• Can/will you use email if that is what the victims prefers?
• What do the staff know about equipment/relay services?
• Do you have a technology or equipment policy?
CHECKLIST (2)

Do you have these either at the shelter or office?

- TTY
- Captel or amplifier for phones
- Phone Signaler
- Videophone
- ADA black kit
- Videophone
ANY QUESTIONS?