From Radio Scanners to Spyware: Technology Abuse & Survivor Safety

Hillsborough County Family Justice Center
NNEDV Safety Net Training – Tampa, Florida

SafetyNet@nnedv.org

Your Relationship with Technology?
- Not on Speaking Terms
- Cordial Working relationship
- Very Intimate

Safety Net:
National Safe & Strategic Technology Project

Stalking, sexual violence, domestic violence, abuse
At National Network to End Domestic Violence Fund
1. Building a network of “techie advocates”
2. Safety Planning – Discussing risks & benefits as technologies evolve
3. Response – Increase systems capacity for survivor-defined prevention & intervention
4. Support Survivors in Self Determination

Important Additional Support:
State Domestic Violence Coalitions
“Technology Advocates”

Beyond Training & TA: Resources & Materials

SafetyNet@nnedv.org
Technology Use…

- Phones
- PDAs
- GPS
- Data
- Caller ID
- Faxes
- Answering Machines
- Email
- IM / Chat
- Internet
- Wireless
- VoIP
- TTY/Relay
- WebCams
- Scanners
- Computers
- Screen Readers
- Refreshable Braille
- Switches
- Magnifiers
- Speech synthesizers
- Alert Buttons

Phone, Internet & Data Intersect

Phone lines carry more than voices:
- People who are Deaf use TTY (teletypewriters) devices to transmit signals across phone lines
- Fax machines transmit images & text
- Dial-up Internet connections – send data packets

High speed Internet connections:
- Buy it with your cable TV package
- Watch movies on the Internet, use webcams
- Make phone calls – via VOIP & IM

Privacy Confidentiality laws & regulations…have a hard time keeping up as tech. rapidly merges

Phone Technology

- harass
- threaten
- target
- stalk
- environmental manipulation
- monitor
- abuse
- groom
- impersonate
- intercept
- surveillance
- victimize

Threats on Answering Machine Tapes & Voice Mail

- If abuser or perpetrator leaves a message, permission to be taped is usually assumed.
- Talk to local prosecutors/law enforcement about their preferred method to report a harassing message left on an answering machine or digital voice mail – learn time limits
- Get answering machines donated & train survivors on use (to screen calls & document harassing messages)

Record-A-Call Phone Handset:
Know laws @ 1-party 2-party consent & notice
Fax Machines

- Always call ahead before faxing
- Check the program Fax settings
- Safety plan around faxing with survivors
- Test Line blocking
- You may be required to enter your real fax number in the header vs. 123-456-7890 or 000-000-000
- Newer fax machines may store data copies of fax

EFax

- Efax services are a third party to your fax machine or email
- Efaxes are susceptible to interception just like email
- Federal Wiretapping laws are more vague
- Service providers may keep digital files

Caller ID & Line Block

- Good for avoiding calls
- Advocacy agencies beware! Even if your # is blocked it may show up.
- Blocking your number: *67 + number
- 800# exception

Phone # Reverse Search
www.AnyWho.com

Caller ID Strategies

- Safety plan with victims/survivors around Caller ID
- Put free line blocking on all/most lines. TEST fax, TTY, cell, home phones with someone who has Caller ID
- Have an organizational policy RE: anonymous call rejection or privacy manager. What do staff do?
- Have policy on survivors unblocking outgoing calls from advocacy center or shelter phone line

Dialing 2-1-1: Information & Referral

- Over 25% of U.S. population has access to 211
- Goal: Dialing 211 will connect customers with resources anywhere in the U.S.
- Learn if 211 is available in your area and how this service can impact victims – go to: www.211.org
- Work with local & state 211 coordinating agencies on privacy and safety issues
- Florida has at least 10 active 2-1-1 call centers
- Hillsborough County 211 served by Crisis Center of Tampa Bay
- See: http://www.211atyourfingertips.org/
Phone Surveillance: Wiretapping, Bugs & Scanners

Wiretapping & Bugs

- Taps can be placed anywhere along the telephone line that runs outside of the house
- Taps allow someone to hear calls or make calls
- There are several ways lines can be tapped for ease dropping purposes
  - Standard line tape with a phone handset
  - An audio recorder with tape
  - A Voice-activated audio recorder
  - A Bug

Illegal Wiretap case

Police said a person could call the phone line and punch in a code that activated a microphone in the hidden device...

Conversations picked up by microphone could be heard over the phone line...

Wireless Phones & Interception

- Radio
  - Basics: using electricity, a transmitter sends sound through the air to a receiver
  - Telephone + Radio = Wireless

Analog vs. Digital

- Analog = Sound Waves
- Digital = Bits of Data

Radio

- Basics: using electricity, a transmitter sends sound through the air to a receiver
- Telephone + Radio = Wireless

Analog vs. Digital

- Analog = Sound Waves
- Digital = Bits of Data
Risks of Using Cell & Cordless Phones

- Losing a call
- Crosstalk
- Loss of legal privilege
- Interception

Not as private as you think.

Interception & Variables

1. Transmitter power (.001 vs 1 watt)
2. fixed frequency vs. spread spectrum (hopping)
3. Analog (broader coverage) vs. digital (010 security)
4. roaming coverage, multimode/dual mode
5. neighbor’s same brand phone...
6. Limited range vs. broad range broadcast
7. Wavelengths:
   - 5.8 Ghz spread spectrum (DSS)
   - > 2.4 Ghz spread spectrum (DSS)
   - > 900 Mhz (older @ 40 diff. channels)
   - > 400 Mhz (outdated cordless)
   - > 43-49 Mhz (baby monitor)

Wireless Scanner Examples:

Radio receiver getting multiple signals (in VHF to UHF range)
Might be portable (rechargeable battery packs), desktop (like regular radio) OR Internet-enabled

Cordless Phones

- ...can be intercepted by scanners, baby monitors, other cordless phones, etc.
- Cordless may not be safe for victims or those working with victims
- ASK victims if they use them
- Limit identifying info or escape details on cordless
- Unplug cordless transmitter after picking up “corded” phone
- Consider proving cheap “corded” phones to volunteers & staff

Cell Phones:

Abuser Use ➔ Safety Tip

- Checks billing records ➔ use safer/donated phone
- Intercepts Analog or Digital wireless phones ➔ use minimal, innocuous, or decoy details
- Uses phone as a listening device ➔ check settings or turn off when not in use
- Tracks Location ➔ talk to carrier & check phone
- Makes it look like victim’s device was used to call/text, when it wasn’t ➔ document victim’s actual actions & explore/investigate how spoof or hijack happened

New Stealth Phone:

- Works as a normal phone you remotely activate
- Phone works like normal until secret number calls target cellphone and never realizes what it does once activated phone switches to stealth mode
- Caller listens in on surrounding conversations phone returns to normal when caller hangs up
- Target is unaware of the stealth activity

The Stealth Phone is built on the success of the spy phone below, it has the same features with one 010 BONUS FEATURE!!! Yea activate appmode remotely...anywhere...anywhere !!!!!!
You can call the stealth phone from anywhere with your own pre determined secret number.
Once called the phone does not ring or show any signs of a call. It switches into app mode.
**Spy Phone Example: Q-phone**

*Q-phone*

**GIVE THIS MOBILE PHONE TO ANYONE AND MONITOR THEM ANYWHERE AT ANY TIME!**

This mobile phone looks and operates like any other mobile phone. It can dial and receive calls like any other mobile phone. However, it has built-in special chips which make it a tracking device that sends data to the Spy Phone Receiver. The Spy Phone will record conversations and store them on a digital (SD) memory card. The Spy Phone can be turned on, monitored, and then returned to normal mobile phone operation. However, it will automatically lock your phone and delete any changes on the Q-phone's display screen. In other words, it appears to be a normal phone. So people who are powerless to take control of the phone.

*Give it as a present to your spouse, kids, employees...know your spouse's behavior when you are away...just push a few buttons and the phone turns into your personal detective...hear everything going on in the vicinity of the Q-phone."

---

**Cellular & Wireless Phones**

- ASK survivors if they use them
- Discuss monitoring risks - settings, location services, phone plans, clones, etc.
- Safety plan about interception points - ask if abuser/perpetrator/stalker works for phone company or law enforcement
- Say ANALOG signals are easier to intercept, DIGITAL Spread Spectrum (DSS) signals are more secure

---

**Cell & Wireless Phones**

- If using to respond to hotline or confidential calls, use sparingly & avoid identifying details – only use digital phones whenever possible
- Incorporate phone donation programs into safety plans (i.e. Wireless Foundation’s Call To Protect & Shelter Help and Verizon Wireless’s programs)

---

**Hotlines & Referral**

- Have/Revise policies on use of various phone tech for on-call advocates
- Negotiate contracts with Answering Services to protect confidentiality, safely dispose of records
- Protect your crisis line billing records (since 800 number bills include #’s)
- Address barriers to access

---

**VoIP – Voice Over Internet Protocol**

- Analog Telephone Adaptor ATA device converts analog signal to digital data → Internet
- IP Phones with Ethernet connector via router → Internet (soon WiFi)
- Computer to Computer (need Microphone, Speakers, etc.)

---

**VoIP: Large growth expected**

- **Cost:** Internet connect as a phone line can save up to 50% over traditional local & long-distance companies
- U.S. subscribers to residential VOIP services growth: 3 million in 2005 → 27 million by end of 2009
- Many companies offer VoIP service: Vonage, AT&T, Skype, Comcast, BroadVoice, SunRocket
- Many different VoIP implementations ~ needs a broadband Internet connection (DSL or cable) but some plans can use a regular telephone
3 Types of VoIP services:
- Fixed: from one location the service is provided
- Nomadic: from any location with Internet access
- Foreign exchange: users in one exchange receive phone calls dialed as local calls in another exchange they selected (e.g. a customer located in Tampa with a Dallas TX local phone #).

2 types of 911:
- Basic 911 = you must tell them your location
- Enhanced 911 = automatically sends your location info. (fixed address or location you registered or real time cell location)

VoIP & 911
- Consumer Advocacy: CT & TX Attorney Generals are suing Vonage for failure to disclose adequately that traditional 911 service is not available to consumers.
- VoIP providers must:
  - Complete the E-911 provisioning process within 180 days of signing up a new customer. Must provide interim 911 service to the geographically appropriate emergency call center.
  - Inform their customers of the capabilities and limitations of their VoIP 911 service.
  - Not market in areas where E-911 service is not available.

Other Safety Risks with VoIP
- Spoofing: Use 3 way calling. Put 1st caller on hold, dial victim 2nd. Caller ID shows 1st # dialed
- Unblocking blocked numbers: local phone company/cell carrier send “Calling Party Number” (CPN) with every call. VoIP software can get system to unblock CPN.
- Tapping: Most VoIP calls are unencrypted across the Internet, making tapping easy
- Call Screening & Call forwarding: User predefines screening list of caller IDs (specific IDs or anonymous calls), then sets how each caller ID is processed
- Call Transferring. Have a buddy call her.
- Call log records all missed, outgoing, incoming & local #.

Victim Safety: VoIP & E-911
- Discuss pros & cons of Registering present address for E-911 service
- Find out what TYPE of E-911 service is provided
  - Service providers may use different strategies or procedures for handling 911 calls.
- If move or traveling, consider re-registering primary address
  - Can take several hours to process – service not immediately available.
- Obtain local emergency direct lines
  - Police, Fire – check on local municipal websites

Victim Safety Strategies: VoIP
- Get a donated cell phone from a local domestic violence shelter to also use for 911
- Keep address & VOIP call-back number nearby
  - If disconnected, 911 provider will need call-back info.
- Check if Burglar Alarm Companies have VoIP compatibility
- If suspect interception, keep a log & document suspicions. (but not on compromised computer)
- Alert law enforcement if you suspect VOIP logging, spoofing/manipulation, interception

Anonymizers: Spoof Cards
Surveillance
Phone Locating & GPS

What is GPS?
- 24 Satellites in space generate & receive radio signals that allow a GPS receiver/chip on earth to estimate its location

If E911 was available in a Pennsylvania town

E911 Info & GPS
- E911= Enhanced 911
- Designed to provide # and exact location of a cell phone 911 caller with GPS Chip in the phone
- In US (1996 FCC rules, & 1999 law) mandated:
  - adding GPS/location chips to new cell phones
  - Phased upgrading of 911 emergency dispatch centers so they can get # & exact location of a 911 cellphone caller via GPS chip
- some regional difficulty rolling this out due to costs

GPS & E911 Safety Planning
- Talk to victims about cell phone location limitations as E911 with GPS is rolled out
- If victim calls 911 from cell phone, she may need to give location in detail
- E-911 & VoIP 911 issues ~ http://www.voip911.gov/
- Victims might want to turn phones off when not in use for location privacy/safety
- If think phone is GPS enabled with location subscription, victim might want to leave phone if flee
- Encourage Cell Companies to provide visible notice that location/tracking is subscribed/on

Locator Services

Locate People & Services

Former AT&T Optional Service: Find Friends for $2.99/month

For Only $5.99 a Month have quick, easy, and secure access to the location of up to 4 Sprint Nextel Phones.

For More Info See: http://www.locatepeople.com

See yours and others current locations
People finder: location of family, friends & co-workers with their permission. Via device or private web site.
Directions. turn-by-turn text directions on your phone
Create Address Book of points of interest

Locator Services

Sprint Family Locator

Former AT&T Optional Service: Find Friends for $2.99/month

For Only $5.99 a Month have quick, easy, and secure access to the location of up to 4 Sprint Nextel Phones.

For More Info See: http://www.locatepeople.com

See yours and others current locations
People finder: location of family, friends & co-workers with their permission. Via device or private web site.
Directions. turn-by-turn text directions on your phone
Create Address Book of points of interest
Location Devices – Spying with Maps

GPS watch & Bio Sign monitor

Monitor Teen Drivers

VEHICLE TRACKING MENU

GPS & Stalking Cases

- Glendale. CA 8/2004: Man arrested when trying to change battery under ex-girlfriend’s car.
- Missouri 12/2005: Police Officer put GPS in ex-girlfriend’s car. Officer was fined.

www.digital-angel.com

GPS & Stalking Cases

- Glendale. CA 8/2004: Man arrested when trying to change battery under ex-girlfriend’s car.
- Missouri 12/2005: Police Officer put GPS in ex-girlfriend’s car. Officer was fined.
GPS Monitoring for Offenders

- Offender wears ankle bracelet & GPS unit at all times
- Information is downloaded & sent to probation/parole officer
- Supervising officer creates “hot zones” (victim’s home & workplace, schools, etc.) where offender is barred from going—officer is notified if location violation occurs
- With “active” monitoring, supervising officer receives immediate violation alerts and can send help to victim
- With “passive” monitoring, supervising officer receives information, typically at the end of each day, and provides no immediate protection for victim(s)

GPS Safety Planning

- Trust your instincts – if you think you are being followed too regularly… there might be a GPS
- GPS device might be small, about the size of a cell phone or possibly in a small box, look for a wire.
- Police might search car for her – advocacy & educational might be needed
- Victims can search the car : under the hood, under the car seats, under the bumpers, in the trunk
- Or get a (new) mechanic to search ($20?)
- A private investigator can do a thorough search, but it could cost $100s to $1000s
- Consider leaving behind car/object if still worried

Hidden Wireless & Wired Cameras

- Examples of hidden cameras

Public Eye In the Sky

Live Web Cams

Univ of Tampa Campus webcam

Example:
- Take picture
- Send image to a friend
- View archived images

Internet Accessed Home Surveillance
“Nanny Cams”

- Security?
- Protection?

• unconsensual recording?
• voyeurism?

Spy Cameras & Sexual Assault

- Voyeurism
- Pornography
- Footage of consensual sex, distributed without consent
- Footage of sexual assault distributed
- Coerced/groomed filming

From the Documentary
RAW DEAL: A Question of Consent

Camera Misuse & Law

Remote Control Spy Car

“Turn play time into spy time!”

Cyclops SR1 Spy Car $199.99
Infrared laser tag game built in Battery operated

- high-res. wireless camera & miniature microphone
- sends real-time audio/video back to its controller
- View & listen on color 1.8” LCD screen or TV screen

Hidden Cameras Safety Planning

- Camera technology evolving - wired, wireless, motion activated, cell phones, upsukiing
- Size, price, capabilities vary widely
- Camera detectors / sweepers offer limited detection (varies by device)

How do I know if one is in my home?

- If remote transmit, there will be a signal.
  - Can buy a device that will tell you if such signals are being transmitted.
- If it is wired instead of wireless... hard to detect except by finding it with your own eyes.
Bug Sweepers & Detectors:
example = Freq. 5Mhz-1.5Ghz

- A Counter Surveillance Probe/Monitor for $1-$3000
- "sniffs" environment for hidden phone, room or body bugs, remote signals, video transmitters, and even wide band frequency hopping or "burst" bugs.
- tests A.C. outlets, phone lines, or suspicious wires for very low frequency "carrier current" signs.
- allows you to listen to telephones or lines for "hot mics," hook-switch bypass and "infinity" bugs, also unknown wires and cables can be tested for wired microphones.
- guards against new devices brought in, remote control activation, or someone tampering with your equipment.
- 24-hour "evidence" recording output stores suspicious sounds while you are away.

Assistive Technology can include…
1. Technology commonly used by general public:
   - Email, IM, computers, phones, PDA’s, etc.
2. Technology created to meet specific needs of people with disabilities:
   - Screen reader, scanner, magnifier, refreshable Braille devices, Braille printers/embossers, etc.
   - Voice synthesizers, talking clocks, switches, TTY & Relay, Video phones, etc.
   - Hands free computer access – speech recognition, point of gaze (mobility), etc.
   - electronic aids to daily living, wheelchairs, hearing aids,
3. Other tools for people with disabilities:
   - Pulley devices to sit oneself up, sticky notes, etc.

TTY & Relay
Communication tools for people who are deaf or hard of hearing

Telecommunication Relay Service (TRS):
- national U.S. service where relay operators provide two-way translation typically between audio/spoken word AND typed text or signed language.

TTY (Teletypewriter) = text telephone
- Communicate by typed text via telephone line to another TTY or to TRS. Also: TDD (Telecommunications Device for the Deaf)

Ways Abusers/Stalkers Misuse TTY & Relay
- Monitor communications
- Impersonate victims/survivors
TTY & Relay

Telecommunication Relay Services:

- survivors use all types: text-to-voice, captioned phone, Video Relay, IP Relay, dial 711, etc.
- TRS provider (operator/communication assistant) must ensure user confidentiality. May not keep records of conversation contents.
- Very limited exception can keep names/numbers dialed: if requested by Speech-to-Speech relay users.

Video Relay (VRS) Example:

Person on Computer with web cam → High-speed Internet → Relay Service Interpreter →

A VRS website using Windows NetMeeting freeware:

TTY, Internet & Relay Safety

- Know & use TTY, Relay, & Interpreter resources
- Do NOT save or print transcript of communications
- Use of 3rd parties & interpreters -- discuss pros & cons of in-person sign interpreters vs. video/remote interpreters
- Potential impersonation -- develop a system to identify a survivor who does TTY or online contact
- Tracks/Records -- TTY machines & history settings, & computer tracks for IP and Video relay, IM logs

IP Relay: Survivor & Advocate Use

To have an IP relay operator call phone # & begin relaying the conversation:

- Go to: IP-Relay.com. Enter 10-digit phone # into “Quick Connect Now” window. Click GO.
- OR
- Open AIM. Create “MyIPRelay” AIM buddy. Then send an IM with the phone # to MyIPRelay.

Ways Abusers/Stalkers Misuse TTY & Relay

- Threaten & impersonate victim/survivors
- Monitor communications

TTY, Internet & Relay Safety (cont.)

- Interception/Security – Email , IM back doors, etc.
- Safety plan about making 911 emergency calls
  - FCC requires that TTYS are compatible with 911
  - TRS must connect survivor using TTY to 911 but may need to ask address.
  - Internet-based VRS & IP Relay should not be used for emergency calls. Not yet required to connect.
  - Be Creative – Pager, etc.
- Support self-determination of communication methods for survivors who are deaf or hard of hearing.
- Create organization practices & policy.
PDAs & Smart Phones

**PDA (Personal Digital Assistant):** small handheld or palm sized computer that might include:
- Email, web browsing, IM, texting
- File transfer, Word processing, camera, music video display
- Screen reader, TTY software program etc.
- Info management tools: Calendar, address book
- Optional phone services, GPS receiver, Data syncs with regular computer

**Smart phones** – a mobile phone first, but also let you email, instant message, surf the Web, listen to music, etc.

Text Messaging

- Also called SMS (Short message service)
- Primary form of communication for teens some send upward of 200 text messages a day
- Take a photo of the cell phone screen to document harassing messages
- Survivors use for help and safety

Networks & Data

- Need Protocol = communication rules - all speak the same language
- Other stuff...Network Interface Cards, Cables, Hub to control traffic

Wireless Networks & WIFI hotspots

- Hotspot = a connection point for a WiFi network.
- How? Access points (small 802.11 radio boxes hardwired into your network) transmit high frequency radio signals up to 100 ft. to talk to your computer’s wireless card
- WiFi hotspots are now in many public places like coffee shops, hotels, libraries and airports.
- Many WiFi hotspots are free & easy to access.

WIFI Risks & Hacks

**WIFI:**
- Packet sniff: views all unencrypted traffic
- Computer Clone: hacks your computer’s ID# from your router
- Evil Twin: misdirect Access Point by using your same service set identifier (SSID), or network name

**Protection:**
- Password, Login & Encryption, Firewalls
**Wi-Fi security ~ access public networks**

1. **Secure your access point login:** Use encrypted login fields for passwords & personal info.
   - WEP (Wireless Encryption Protocol) is weaker
   - WPA (WiFi Protected Access) is stronger
   - 64 < 128 Bits
   - Lock down Wi-Fi network access by MAC (Media Access Control) address ~ on your wireless card

2. **Secure your session & data after logging into an access point:** Use a client firewall & VPN tunnel

3. **Know your service provider’s security policy**

---

**Bluetooth Personal Area Network**

- Bluetooth chips replace cables between devices
- This wireless technology uses a globally available frequency band (2.4GHz)
- Short-range < 30 feet
- Universal bridge ~ integrates devices ~ communicate with mobile devices

---

**Phones, PDAs & Computers with Bluetooth**

**Freedom Scientific’s StreetTalk for PacMate: GPS**

- Like many GPS, can plot routes & download maps ahead of time or in real-time
- Provides turn-by-turn Braille or speech announcements
- Can use Bluetooth to be 30 feet away from user, e.g. on a guide dog harness
- Abuser can misuse it to track a victim’s every move.

---

**Bluesnarfing**

The theft of information. This includes, your contacts, passwords, text messaging, without leaving any evidence of the attack.

---

**Bluejacking**

Temporarily hijacking another person’s cell phone by sending it an anonymous text message.

Used to flirt.
**Bluebugging**

Most Dangerous!

- Secretly turn on another person’s phone and make it call you.
- The attacker could then place calls to other numbers via that person’s phone.

**Calls can be intercepted and the phone can be used as a listening device.**

**Tips to Enhance Bluetooth Security**

- **Set the device to "hidden".** Personal devices like headsets can still connect to the phone, but intrusion is much more difficult since the hacker will have to know the Bluetooth address before establishing a connection.
- If a user wants absolute security, they can simply "switch off" the Bluetooth functionality of their mobile phone. This will not affect other functionalities of the phone.

**Benefits and Risks of Using Computers & the Internet**

- Amazing resources on the web for victims and advocates if accessed safely
- Discuss computer safety planning if you give a VAW/DV/SV website address
- It is NOT POSSIBLE to clear all “footprints”
- Assess credibility of information
- Look at which state(s) the info covers

**Internet History, Temporary Internet Files (cache) & Cookies**

- History

**Severe Limitations of “Window Washers”**

Are You Being Watched?

Your Internet activities are being recorded. Every picture you've seen is copied to your hard drive, every website is recorded in a hard to find file in Windows. Every website you've visited is added to your drop down list. Your homepage could be changed and you can be tracked from anywhere.

Clean your Internet Tracks everyday. You need to start now! Don’t let other people see what is on your computer.

Click Here To Protect Your Privacy Now!
**Adware Vs. Spyware**

- **Adware (AKA Pestware):** client-side ad serving software that delivers advertising to consumers, and might also profile users' Internet surfing and shopping habits. This is normally downloaded by the user as part of a free software bundle via the Internet.
  - Symptoms: sluggish system, lots of advertising pop-ups

- **Spyware (AKA Malware, Surveillance Software & Hardware):** software program or hardware component that helps an unauthorized third party (such as an abuser) to gather information about the user's computer use without his or her knowledge or consent.
  - Symptoms: often none, they typically run in stealth mode so user never knows it's installed

**ComputerGOD: Makes Remote Computer Talk**

- "...the most powerful remote surveillance & control program on the market."
  - Silently records all keystrokes, websites visited, email received, passwords, instant messages, details of applications & windows opened, & snapshots of the screen taken periodically.
  - Control most functions of a remote computer: you can restart, shutdown, & logoff a computer, send chat messages, control the remote computer's desktop & mouse, transfer files, & make the remote computer talk any words.
  - Remote installation capable. Designed to allow a user to monitor & control multiple computers.
Screenshots of My Email

I think I am being abused by my husband. I need to talk to someone, but I have a hard time getting any time alone. I think I need to come to a shelter - can you tell me where you are located so I can bring my 2 children to a safer place?

Thank you,
Jane Smith

Loverspy Creator & Users

Indicted August 2005

- Disguised as puppies & flowers e-greeting card
- Marketed at $89 to “catch cheating lovers”
- Creator indicted for manufacture, sending, & advertising a surreptitious interception device. Also unauthorized access to protected computers.
- Violated US federal computer privacy laws = illegally intercepting electronic communications

Warning: IF spyware already on computer... THEN risk of imperfect or no detection by later installing countersurveillance, firewalls, anti-virus programs

Keystroke Logging Hardware

To install the hardware, you simply plug the keyboard cable into the back of the device you want to monitor and turn it on. The device logs all keystrokes and sends them to a remote computer via a network connection. This can be used to track a person's keystrokes and virtually any other data they type.
Keystroke logging keyboards

Protections & Security:
1. Anti-Virus & Anti-Spyware software – keep updated definitions
2. Install Firewalls – to filter incoming data packets, ports, protocols, etc.
   • Software – ex: free Zone Alarm
   • Hardware – ex: Linksys Cable/DSL router <$100
   • Network wide (LAN’s, WAN’s, VPN’s) & home use
3. Promote use of encryption (scrambles data – need key) & authentication (passwords, passcards, etc) for sensitive data. Especially for wireless networks.

Some Anti-Adware & Anti-Spyware Programs (Sniffers)
For Adware, use (in order of effectiveness):
- Giant Anti-Spyware giantcompany.com
- Spy Sweeper www.webroot.com
- AdAware www.lavasoftusa.com/software/adaware
- SpyBot Search & Destroy www.safer-networking.org/en/download

For Spyware, use:
- XBlock (freeware version) http://www.xblock.com/installer.shtml

Note: NONE of these programs can guarantee detection & removal of adware & spyware. For that, you must reformat the hard drive

Safety Tips for Advocates
- Regularly ask survivors:
  • “Do you use a computer?” and
  • “Does the offender have onsite or remote access to it?”
- Encourage using a “safer” computer at the library or elsewhere
- Discuss risk from tech savvy stalkers
- SPYWARE trumps all

Safety Tips for Survivors
- Create a new email account on a safer computer
- Change passwords frequently, don’t use obvious ones
- Don’t open attachments from an unknown source
- Install a personal firewall & anti-virus protection
Password Safety

- Change your password often
- Don’t use something obvious
- Incorporate numbers, letters, and characters
- Don’t tape it underneath your keyboard
- Don’t share it or let someone else use your computer when you’re logged in
- Alphanumeric Password: N4XF6

Website Accessibility

Safety & Spyware

- Does your organization have one?
- What sort of information does it provide?

Why Don’t We Publish this Info on the Web?!

- It’s vital to get tech safety information to victims!
  But we need to do it in ways that do not give ideas or explicit instructions to abusers and perpetrators.
  Example: “There are cell phone settings that can be used to monitor you… so it may be safer to turn cell phones off when not in use”. We don’t publish details about “silent mode + auto answer”.
- Please do NOT post explicit tech information on the web, or publish in newsletters that will be posted on websites.
- See NNEDV website (www.nnedv.org) and/or contact Safety Net Team (safetynet@nnedv.org) to discuss further.

Make Your Website Safer

- Minimize info. that educates abusers
  - Encourage use of safer computers
- Don’t post personal info. without consent
  - No email addresses
- Support informed choices: on every page have an alert to survivors about online tracking & safety risks

Web Forms vs. Email Addresses

The safest way to reply to me is by:

- **Enable Informed Choices**
  - Phone
  - Is it safe to leave a message?
    - yes
    - no
  - Email
  - Mail

Web forms don’t place a copy of the sent message in the sender’s email application

Website Safety Alerts

- There are hundreds of ways that computers record everything you do on the computer and on the Internet.
- If you are in danger, please try to use a safer computer that someone abusive does not have direct access, or even remote (hacking) access to.
- It might be safer to use a computer in a public library, at a community technology center (CTC) www.ctcnet.org (national directory), a trusted friend’s house, or an Internet Café.
- Email is not a safe or confidential way to talk to someone about the danger or abuse in your life, please call instead.
- Traditional “corded” phones are more private than cell phones or cordless phones.

Safety alert: computer use can be monitored & 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.

SafetyNet@nnedv.org 115

SafetyNet@nnedv.org 116

SafetyNet@nnedv.org 117

SafetyNet@nnedv.org 118

SafetyNet@nnedv.org 119

SafetyNet@nnedv.org 120
SafetyNet@nnedv.org

**What is Web Accessibility:**

- "The power of the Web is in its universality. Access by everyone regardless of disability is an essential aspect."
  - Tim Berners-Lee  Inventor of the World Wide Web
- Web Accessibility on the Web is about Universal design.
  - The design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design.

**Make Your Website Accessible**

Screen readers can speak the content of Web pages aloud to a survivor who is blind or has dyslexia.

**Your Website - Accessible to all?**

- When the screen reader gets to a picture:
  
  ![HELP HELP.png](help.jpg)

  If you put an “alt” code text description of the image, a screen reader will say: “Click here for help”

  `<img src="help.jpg" alt="Click here for help">`

  Without that text description, the screen reader will only say aloud “image”.

**Safety Issues in Online Communication:**

- Email
- IM & multimedia
- Counseling

**Online Advocacy: Benefits & Risks?**

<table>
<thead>
<tr>
<th>Potential Benefits:</th>
<th>Significant Risks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility</td>
<td>Privacy Breaches</td>
</tr>
<tr>
<td>No child care/transportation</td>
<td>Interception (Spyware)</td>
</tr>
<tr>
<td>No worry about being recognized walking into a building</td>
<td>Impersonation</td>
</tr>
<tr>
<td>Online translators or language specific support</td>
<td>Harassment</td>
</tr>
<tr>
<td>Geographically remote locations, rural folks</td>
<td>Helpfulness (untested)</td>
</tr>
<tr>
<td>Virtual support group option across communities, towns: decrease isolation, increase support for minority groups in homogenous communities</td>
<td>Assessment Difficult</td>
</tr>
<tr>
<td></td>
<td>Organizational Liability</td>
</tr>
<tr>
<td></td>
<td>Legal Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Duty to be Available – Technology Breaches</td>
</tr>
</tbody>
</table>

**Email Privacy Tips for Survivors**

- Have more than one email address - work, home, anonymous, online ordering, etc.
- Create new email accounts the abuser doesn’t know about. Use new secret passwords - no birth dates.
- Ask friends/family to not share new email
- Consider having a separate account for abuser emails regarding custody & visitation
- Use safer computers when accessing new email
Advocate Email Use

- 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.

Tracing Emails - It Can Be Done

- Internet Service Providers (ISP) assign a user an IP when they log-in (Dynamic or Static IP address).
- ISP keeps subscriber info (name billing) and connection logs of who used an IP address & when.
- Emails Header info. is crucial to tracing: delivery path info...mail server info, IP addresses, dates & times.
- Computer Investigation/forensics & threat management units can trace all of this.
- OR you can go to WHOIS info: www.samspade.org

Example: Email Roadblocks

- Forged headers,
- Anonymous Remainers – remailer strips header from original email and inserts a different header and resends the email – sometimes routed through 3 remailers.
- ISP’s that don’t retain records for long,
- What else??

(IM) Security Threats

- IM can transfer text as well as files such as worms or spyware.
- IM can open you up to backdoor Trojan horses & viruses by opening a listening port on your computer, bypassing your firewall.
- Once your firewall has allowed IM in, the connection stays open – hackers can get in.
- Messages are not private. Your messages can be viewed by others.

Multimedia Instant Messaging

- Instant text messaging with people on your buddy list. Access to a universal address book. Send/receive IMs from your mobile device.
- Audio connect and phone: Use Voice Chat talk to up to 20 buddies at a time. Activate a free phone line to get a local phone number with unlimited incoming calls, caller ID and voicemail delivered to your mailbox.
- Video chat - its like a high-quality video conference. Plug in your webcam and look at each other while you chat.
- Can increase accessibility: Might be used for signing between two people who are deaf.
- Use IM via a web browser interface. *to protect against trojans, this is safer IMing.
Encryption Tools

Email
(PGP) Pretty Good Privacy
http://www.pgpi.org/

Instant Messaging
1. After download IM programs
2. Download Gaim: multi-protocol IM client
3. Add Off-the-Record Messaging (OTR) – then have private conversations with: Encryption, Authentication and additional security

Example: Crisis Center of NE Texas

1. Create user ID & password
2. Leave request
3. Sign back into website to get response

Online Advocacy

- Many risks re: “protected conversations”, organizational liability, etc.
- Have a policy
- Discuss safety & confidentiality risks and alternative options before considering
- Weigh different risks per method (email, discussion software) for one-on-one contact vs group, closed vs. open.
Virtual “Speak Out” Safety

- Talk to survivors about the ways that they use blogs for empowerment and healing
- Safety plan around identity and online searches
- Discuss ways that blogs are used to harass or abuse – comments, monitoring without survivors knowledge, etc.
- Who has access to your story?
- Online name linked to real identity?
- Archived by search engines?
- Who moderates?  

Example of Blog Posting


Online Social Networking

- Since 2001, online social networking has expanded to over 300 websites, including:
  - Friendster, MySpace, Facebook, LiveJournal
  - Tagged, Tribe.net, Xanga.com, Meetup.com
- Very popular, huge growth in use.

Online Forums

“Victims reaching out to other victims”
What are the Risks?

- Your friends’ friends’ friends will be able to see your info and become part of your social circle
- Personal info posted online is not private—like a billboard on a highway
- Predators troll online communities to find victims
- Family, teachers, coworkers, coaches, employers can all access your info

SAFETY TIPS

From MySpace & Tagged

Be a Savvy User

- Use code phrases
- Think 2x before posting personal info
- If you use your dog’s name as a password (which you shouldn’t) – don’t post your dog’s name online!
- Think before accepting new “friends”
- Think before posting photos - Adults need to model

Data All Over The Web: Abuser Access & Survivor Safety

Data All Over the Web

- Directories & Search Engines
- Maps & Hybrid data (GIS)
- Court & Government Sites
- Individual and Organization Web Pages
- Information Brokers

Combining networked databases, tracking devices and increasing commerce/services on the web = CHALLENGES for survivors

Individual & Organization Sites
ZabaSearch ~ Free Databases

Births
Adoptions
Courts
Marriages
Sex offenders
Military
Schools
Property
Vehicles
Licenses
Campaign $
Maps: Satellite & Hybrid Data

Latitude & Longitude of NNEDV

SE DC ~ Towards NNEDV

NNEDV closer

NNEDV office block

Directories & Search Engines

people, place, phone
Shrinking Anonymity
Access to Databases:
directories, courts, taxes, voter, Jiffy Lube, car repair, grocery store, video rental, etc.

Social Engineering
- Clever manipulation of the natural human tendency to trust
- Weakest link in security for any system is our willingness to accept someone at his/her word
- Most common method of gaining access to passwords
- Limit who has access and knowledge of passwords

Pretexting & Data

Social Engineering
- Clever manipulation of the natural human tendency to trust
- Weakest link in security for any system is our willingness to accept someone at his/her word
- Most common method of gaining access to passwords
- Limit who has access and knowledge of passwords

Pretexting
- A police officer seeking revenge against a former girlfriend hacked into the woman's e-mail account, assumed her identity at an online dating service and contacted 70 men, inviting some of them for rendezvous at the woman's home.
- The woman discovered the scheme when male strangers began appearing at her house, claiming she had solicited their visits via Match.com.

Information Brokers
...Beware of Pretexting
Amy Boyer Case

1. Online broker Docusearch, obtained information @ Amy Boyer with a pretext calls. Sold Amy’s SSN & place of employment to stalker.
2. Stalker then found and killed Amy
3. Family sued online broker. NH case established:
   - Gathering personal info. by pretext violates consumer protection laws
   - Investigators/brokers must exercise reasonable care in disclosing 3rd party personal info to a client

Take Reported High-Tech Stalking Incidents Seriously

- 54% of femicide victims reported stalking to police in the year before they were killed by their stalkers.
- 46% of attempted femicide victims reported stalking to police in the year prior to the attempted murder.
- Recidivism rates in stalking cases are around 60% — Even after a criminal or civil justice intervention!

(Stalking and Intimate Partner Femicide, McFarlane et al., 1999)

If Survivor wants to Report Crimes

- time may be limited for some evidence
- Safety Plan (Technology Safety Plan)
- Document & Save (Tips for Victims of High Tech Stalking – Log Sheets)
- Survivor can check cars, test situation, but do not remove or delete evidence

Investigation Issues

- Believe the victim even though seems “sci-fi” 😊
- Identify & Work with Technology Crime Unit
- Preserve evidence asap (letter to ISP, digital voice mail, etc)
- Work with victim to document & make sure her/his logs contain appropriate information for investigation
- Explore training resources for High Tech Investigations
- Will the investigation of a tech crime impact other important parts of her/his life? (taking computer)
Preserving Evidence - Subpoenas, Search Warrants, Court Orders

- Seize computer
  - Internet history
  - Bookmarks
- Look for unknown accounts
  - Hotmail
  - Yahoo
  - Geocities
- Credit Card Purchases
  - Pornographic web sites
  - Dating web sites
  - Software purchases
- What else?

DOJ/NIJ Recommended Resources:

- Digital Evidence in the Courtroom: A Guide For Law Enforcement and Prosecutors (Jan. 2007)
- Investigations Involving the Internet and Computer Networks (Jan. 2007)

Victim-centered processes

Survivor-led safety planning

- If reported, is victim ready for media coverage? Will it impact a survivor’s safety and ability to assist in a prosecution or perpetrator accountability steps?
- Will investigating a cybercrime impact important parts of her life? (e.g., taking survivor’s computer)
- Work with the survivor to identify what will best hold perpetrator accountable without further victimizing, endangering, or negatively impacting her/him
- SAFETY SAFETY SAFETY

Data Safety Concepts

Challenges of Digital Data

- Note: Internal paper use is almost equal to **SECURE** internal computer use of data
- Combined Data – too much info in 1 place
- Exported or Shared Data – lose control
- The more data that is collected, shared, & combined, the higher the risk for victims

Between Feb 2005 and June 2006, over 84 million Americans have had their personal info compromised
RFID Credit Cards & Toll Passes
Radio Frequency Identification

RFID is an automatic data capture technology that uses tiny tracking chips affixed to products.

Why Confidentiality, Privacy, Data Safety?
- Victims won’t come to our doors
- Info could get to Perpetrators, Community, etc
- Inappropriate info could end up in wrong place
- Info in records could get into hands of abuser’s attorney…
- FOIA, Discovery, Liability, etc

Information is Power: Theory & Practice
- Core Value of Confidentiality
- We all choose who we’re willing to tell what – it’s normal & important
- We don’t need to know everything to do good work and help victims
- As a survivor, it’s my personal information, I hold the power of my own info

Information is Power: Theory & Practice
- We want to increase her/his access to advocacy, justice, & services
- We want to save ourselves work 😊
- Sharing data has some benefits, but MANY risks
- Sensitive & privileged info must be protected

Things to Ponder
- Victims can also be defendants – protecting their location information can save lives
- Perpetrators can work in the system
- Hackers are adept at getting into systems
- 70% to 90% of security breaches are Internal

1 study: 81% of security breaches originated internally, another 13% percent came from ex-employees, 6% from external hackers

Data Terms
- Personally Identifying
- Client Level
- Aggregate
- Informed Consent
Victim Data Analysis

1. Why: Purpose of Collection/Sharing
2. Who has Authorized Access
3. What is the Content of the Record
4. Where is the location of the Data
5. How Long will the info be stored?
6. How Secure is the Data
7. Who else wants the info (Function Creep)

Data, Stats & Security

- NO confidential client names on any computer connected to the internet
- Store any confidential info on a separate computer in a locked space, or use a removable hard drive to lock away data
- Install a software Firewall (even a free one)
- Keep your Antivirus software up to date
- NEVER open attachments from unknown sources

PRIVACY
Includes a survivor’s right to own her/his stories...

- impacts safety & healing
- influences quality of life
- chances of revictimization

Data Collection

**PRIVACY POLICIES**

- Have them!
- Develop privacy & technology policies OR add tech issues to existing policies
- Include who has access to what, when purged/deleted, security, etc

Use Technology & Data Practices that Support & Create Safety
Incorporating Your New Tech Awareness
Next Steps: Key Questions to Consider

1. How can you share this information within your organization?
2. Who else do you need to bring into the conversation?
3. What will be easier to implement?
4. What will be more difficult to implement?
5. How does FJC co-location make it easier to implement, or harder?

This project was supported by Grant No. 2004-WT-AX-K082 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this presentation are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.