## *PART 6 - TECHNOLOGY SAFETY PLANNING AND BEST PRACTICES*

If you are working with a client who has already been a victim of cyber sexual abuse and/or technology abuse, or expresses fear that his or her abuser may use technology against them, use this section to guide your client through technology best practices.

While working through safety planning with your client, it is critical to consider the safety implications of removing or limiting the abuser's access to their technology. If the abuser realizes that they have been "caught" and/or no longer has access to information about your client, this may escalate the abuse. Always do technology safety planning in the context of a comprehensive safety plan. If you need assistance working with your client to create a comprehensive safety plan, consult Part 7- Resources of this Manual for referrals.

This section will start by covering some general technology and online safety tips that can apply to all digital media, as well as some preventive measures. It will then go on to discuss certain media, devices, or accounts in more specific detail.

### I. General Safety Tips: The "Digital Breakup Plan"

If your client is considering leaving an abusive relationship, there are things he or she can do ahead of time to try to mitigate the damage that his or her abuser can do with technology. Use this list as a starting point for your client's "digital breakup plan":

- Change all passwords on all accounts to secure, unique ones that cannot be guessed by the abuser. Help your client try to remember every account that they may have online, including e-mail, social media, "cloud" storage, school, banking, and even shopping accounts (which may have stored credit card and address information).[224]

- Do not set passwords as children's names, important dates, or other personal things that might be easy for someone who knows your client to guess. The most secure passwords are those that contain only random strings of letters, numbers, and symbols.

- Along the same lines, do not use answers to password-reset security questions that the abuser knows. Give fake answers to security questions, or better yet, use random strings of letters, numbers and symbols as these answers as well.

- Do not use the same password for every account; if the abuser manages to get the password for one account (e.g., through keystroke logging), then they will have access to all your client's accounts. Many people use the same password on all their accounts because it is too hard to remember so many different random and unique passwords. Instead, a free online password manager allows you to create one secure, unique

[224] For guidance through common online accounts, *see Coach: Crash Override's Automated Cybersecurity Helper*, CRASH OVERRIDE, http://www.crashoverridenetwork.com/coach.html (last accessed Mar. 21, 2019).

password to log into the manager, and then the manager creates and saves random passwords for every other site.[225]

- Turn on two-factor authentication for every website and account that offers it, especially the password manager. Two-factor authentication (2FA) requires both a password and a one-use code sent to a cell phone or other device to log in. Using 2FA means that someone can only log into your client's account if they have physical access to their cell phone. If 2FA is available on an account, it is usually turned on through the settings tab. Ensure that the phone the codes will be sent to is a safe one that the abuser does not have physical access to.

- Enable firewalls and install antivirus and anti-spyware software on all devices.

- Have your client's computers and electronic devices analyzed for spyware. There might be spyware installed on your client's device if it is behaving strangely — e.g., running slowly, draining the battery too quickly, crashes more often — or if the abuser seems to know information about the client that they should not know. This manual contains some information about detecting spyware, *see supra* Part 6-Technology Safety Planning. Your client can also take the computers/devices to a professional to have them analyzed.

- Have your client secure their home WiFi network by resetting their password.

- Have your client search their belongings for GPS tracking devices (e.g., car, purse). They can also ask law enforcement for help. Have your client search their home, or ask law enforcement to search their home, for hidden cameras, particularly in areas that the abuser has had physical access to, or objects in the home that were gifts from the abuser to the client or family members. Note that "camera detectors" are effective in detecting wireless cameras, but not those that are hardwired.

Of course, tech tips alone will not keep your client's information safe, if the abuser has access to non-digital sources of information. Brainstorm with your client about how else their abuser may be able to get information or monitor their activities. Does the abuser have access to the client's home? Mail? Workplace? Do they have children or mutual friends who may share information?

## II. Securing Cell Phones and Tablets

Cell phones (and tablets with Wi-Fi or data plans) are a very common source for an abuser to collect all sorts of information about your client, including their location, their communications, and their photos and videos. Spyware installed on the device is one way for an abuser to secretly monitor your client, but even without spyware, your client's cell phone can broadcast a lot of dangerous information about them.

[225] LastPass is a helpful free online password manager, https://www.lastpass.com/. LastPass also allows your client to store their fake answers to security questions, as discussed above.

- Put a passcode on the phone, so that even if the abuser has physical access to the phone, they cannot open it up to access the information.
- Turn off automatic login and/or saved passwords, so that if someone has access to the phone, they cannot log into online accounts with sensitive information.
- Turn off location sharing and Bluetooth when not in use.
- Go through the phone's privacy settings: both the general privacy settings, as well as the individual settings for all installed apps.
- Review the apps that are installed on the phone, and delete any unfamiliar ones.
- Check if the abuser has access to the client's phone account (e.g., on their family plan). Consider removing the abuser from the plan, or change the password to the account.
- Be aware if your client's phone is acting strangely, which may indicate spyware or other malicious tracking software:
    - Running slowly, getting hot, battery draining;
    - Spikes in data usage;
    - Takes longer to shut down;
    - Screen lights up when not in use;
    - Clicks or sounds on calls;
    - Incoming calls on bills that user did not receive.
- If malware or spyware is discovered, be careful about transferring content to a new phone, which will also transfer all the malicious content.

For iPhones specifically:

- Enable Touch ID or a passcode.
- Check your client's iCloud and Apple ID, change the passwords, and delete any e-mail addresses that your client does not want to have access to the account.
- Consider turning off the setting to automatically back up photos, mail, contacts, etc. to iCloud.
- Turn off the "Find my Phone" feature, which allows someone to find the location of the phone by logging into iCloud.

- Turn off Family Sharing, or turn off the feature that shares the phone's location with family members.

- Disable "Find my Friends" feature.

- Ensure text message forwarding is turned off and texts are not being forwarded to another phone number.

- Remove any "trusted devices" you do not recognize.

- Turn off Location Services for any apps that are not currently being used.

- Set up the privacy settings of individual apps to control what information on the phone each app can access.

- Be very cautious about "jailbreaking" the phone, which will remove important security features that prevent malware and spyware.[226]

## III. Computers, E-mail, and Online Browsing

If your client uses a desktop or laptop computer (which may be easier or harder than a phone for the abuser to have physical access to, depending on their living situation), there are additional safety steps to discuss with your client.

As computers are more likely to be shared by multiple family members than phones or tablets, especially if the parties live together, it is critical to weigh every safety step against the possibility that limiting the abuser's access to the computer and/or wireless network will tip the abuser off that the client is preparing to leave the relationship, and may be more dangerous than leaving the computer alone. If the abuser has physical access to your client's computer, and/or is on a shared network with your client, and it is unsafe to limit this access, your client may wish to consider using a safer device, such as a library computer, for any communications and/or web browsing that they wish to keep private.

If it is safe for your client to take precautions on the computer, follow these safety tips:

- As discussed in Section I above, change all online passwords and enable 2FA. Enable a password lock on the computer itself, and remove the abuser's login profile from the computer.

- Password-protect the wireless network, and remove any of the abuser's devices as authorized devices on the network.

[226] For more detailed iPhone safety tips, *see iPhone Privacy & Security Guide*, Technology Safety, NATIONAL NETWORK TO END DOMESTIC VIOLENCE, https://www.techsafety.org/iphoneguide/.

- Enable firewalls, install anti-spyware/anti-virus software, and always keep the software up-to-date.[227]

- When reading e-mail, do not open attachments from unknown senders. When browsing, do not visit unknown websites or click on unknown links.

- Turn off cookies in the browser settings, and regularly delete cookies and search history. Many browsers also offer "private" or "incognito" browsing which does not record the browsing history and deletes cookies after the browsing session is closed.

- If your client's abuser seems to know too much about your client's computer activity, then there is a possibility that the computer has been compromised, for example by "keylogging" software, which records all the keystrokes that are made to that computer. With an active and fully updated antivirus program running, it is harder for keyloggers to be installed, but if your client suspects one and has a PC:

    - Open the Task Manager and check the Task Manager window for suspicious programs running; search the names of unknown processes on the Internet to see if they might be malicious.

    - In the Start menu search bar, type in "msconfig" and press enter. Go to "Startup", and see if there are any suspicious programs that are configured to start up when the computer boots. If a program looks suspicious, search for its name on the Internet to see if it might be malicious.

    - The program may be able to be uninstalled just like any regular program using the Control Panel. Once uninstalled, run a scan with antivirus software to ensure that it is completely gone. However, if the keylogger is very malicious, regular uninstallation may not work. Your client can consult with an IT or help desk professional for assistance in removing the keylogger, or it may require the operating system to be completely reinstalled.

    - If it is a desktop computer, look at where the keyboard cable connects to the tower. If there is a device plugged in between the keyboard cable and the tower, it might be a hardware keylogger.

## IV. Social Media Accounts

Social media is a goldmine of information that your client may be inadvertently sharing with their abuser. Descriptions of specific social media sites and the ways they can be used are discussed more in-depth earlier in this Manual, *supra* Part 3- Description of Relevant Social Media/Applications and Associated Abuse. In general, your client should take certain precautions on all their social media sites (in addition to changing all their passwords and enabling 2FA):

[227] A reputable and free antivirus program for both PC and Mac is Avast, www.avast.com.

- Turn off location services.

- Check all privacy settings. Set up notifications to get a message if someone tags, messages, or comments on your client's posts. Set up a notification to let your client know whenever someone has logged into their account.

- Be careful about "checking in" to locations, as this will allow the abuser to track your client's location.

- Beware of "geotags" on photos, which is hidden data that records the GPS location of where the photo was taken. Sharing that photo on social media may expose your client's location even if they do not explicitly "check in" somewhere.

    - On an iPhone, you can turn off geotags in Settings/Privacy/Location Services/Camera. To remove geotags from photos already taken, use a photo privacy app from the App Store.

- Do not link social media accounts with e-mail accounts.

The victim may wish to block or unfriend their abuser. Their counsel should discuss with them whether this is safer or whether it will trigger the abuser to retaliate. It also means that the victim will no longer be able to see what the abuser is sharing about them, which may make it harder to react. In addition, their counsel may lose access to evidence that you may need for a current or future legal case. If the victim decides to block or unfriend the abuser, counsel should consider whether there are ways to preserve the evidence beforehand.

## V. Credit Cards and ID Theft

This Manual does not focus on identity-theft issues. However, identity theft is definitely a tactic that a digital abuser may use, so we have included a few tips for instances where your client fears that their abuser has their Social Security number or may try to steal their identity and open fraudulent accounts. You can begin by having your client run a credit report on all three of the credit reporting agencies (Experian, Equifax, and Transunion). Everyone has the right to get one free credit report from each of these agencies once a year, for a total of three free credit reports a year.

A victim should use www.annualcreditreport.com to request their free credit report. There are other websites that purport to be free, but many of them require a trial account to be opened, or for "credit monitoring services" to be purchased.

Be aware that running a credit report using a confidential address may then make that address become part of the credit report, and if an abuser can access the credit report, the abuser will then have the confidential address. Instruct your client to use a prior, known address to run the report, or have them register for a confidential address if that is offered in your state (it is offered in New York).

If any of the credit reports show fraudulent activity, your client should:

- Call the fraud department of all their accounts, report the fraud, and follow the directions given by the service rep. This may include closing the accounts, getting new cards, changing passwords and PINs, etc.

- Contact each of the credit reporting agencies to put a "fraud alert" on their file.

- Report the ID theft to FTC and local police; share the police report with the credit reporting agencies.[228]

## VI. Nonconsensual Pornography: Images and Videos

Discuss with your client whether he or she is aware of any intimate images or videos of themselves that their abuser may use to threaten, extort, or harm them. Your client may have shared intimate images voluntarily during the relationship. However, his or her abuser could also have obtained private photos or videos without your client's knowledge or consent. Images can be captured through hidden cameras, by recording or screenshots through Skype or another video chat, or by accessing your client's photos, either from the physical device where they are saved, or from "cloud" storage. If you are counseling a client who reveals that they are considering sharing intimate photos with a partner, you could suggest that your client take precautions, such as avoiding showing any identifying features (e.g., face, tattoos, birthmarks), using a neutral non-identifying background with dark lighting, or adding a filter to the photo.

By following the general safety steps outlined above, your client may be able to prevent their abuser from obtaining intimate images. However, if your client knows that the abuser already has intimate images, there are a few steps that may help prevent the abuser disseminating these images, or at least alert your client quickly if the images have been shared, so that they can take swift action.

- Have your client do a Google search, and then set up a Google news alert, for their name, so that they get an e-mail whenever a new hit is found.

- Facebook has launched a program in which people can voluntarily share the intimate images that they fear might be disseminated, and Facebook then converts those images to a digital code to prevent someone else from uploading and posting the photo. Discuss with your client whether this is something they are comfortable doing. This project is discussed more in-depth at https://www.techsafety.org/blog/2018/7/10/facebooks-proactive-approach-to-addressing-nonconsensual-distribution-of-intimate-images.

- Discuss with your client their legal options if the images do become public, including how to preserve the evidence for later legal action. Legal remedies against the abuser are covered in Part 1- Criminal Legal Remedies for Victims of CSA and Part 2- Civil

[228] The FTC has a comprehensive document called "Identity Theft, a recovery plan" that covers the steps to take in more detail. *IndentityTheft.gov*, FEDERAL TRADE COMM'N, https://www.identitytheft.gov/.

Legal Remedies for Victims of CSA and evidence collection and preservation is discussed in Part 4- Evidence Collection of this Manual.

## VII. Detecting Spyware

Spyware is any computer program or hardware that enables an unauthorized person to monitor communications, location, and other data, often without detection. Dozens of programs and applications exist that allow users to track another person's whereabouts, take photos, record ambient audio, and remotely wipe or lock the device.[229]

Spyware is difficult to detect and remove because it is often hidden. The abuser may be able to download spyware secretly and obscure its presence on a phone or computer. In addition, there are several "dual-use" applications that are "designed for legitimate purposes, such as anti-theft tracking apps, 'Find My Friends,' emergency response apps, parental control apps, and others," but that can be used to commit intimate partner violence.[230]

Preventing spyware from being downloaded can be difficult. Many apps have functionality to hide their icons from a phone's screen. Be wary of phones that have been "jailbroken" or "unlocked," as this removes security features that prevent spyware from being downloaded. Educate your children and family members so they do not inadvertently install spyware.

While there is no sure way of detecting spyware, the following are things clients should look out for. Law enforcement and advocates can help if spyware is believed to have been downloaded.

- Be aware if your phone or computer:
    - is running slowly;
    - is getting hot;
    - has a quick-draining battery;
    - has spikes in data usage;
    - takes longer to shut down;
    - lights up while not in use;
    - clicks or has odd sounds while on calls;

[229] RAHUL CHATTERJEE ET AL., *The Spyware Used in Intimate Partner Violence* 9 (2018), https://www.ipvtechresearch.org/pubs/spyware.pdf.

[230] DIANA FREED ET AL., *"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology* 6-7 (2018), http://www.nixdell.com/papers/stalkers-paradise-intimate.pdf.

- has any new or suspicious hardware, like a keyboard, cord, or USB drive; or
- has incoming or outgoing calls that you do not recognize.

- Be aware if your abuser knows things that you've only told people via e-mail, text message, or phone calls (ex: your whereabouts, your search history, etc.)

Individuals should be careful about looking for and removing spyware because it could be dangerous to alert the abuser of your suspicion. Use a computer or phone at work, a public library, a community center, an Internet café, or a friend or family member's computer to perform searches or send e-mails to avoid detection by the abuser. Continue to use your device for innocuous tasks, like checking the weather, so your partner does not get suspicious.

Removing spyware is challenging. The only sure way to remove spyware is to discard the device and get a new one. Short of this, wiping the device to its original factory settings is often effective. It is suggested that clients back up their device before resetting it, as this can be helpful to law enforcement personnel to have a record of the device's activity. It is important *not* to download the contents of the backup to a new or recently wiped device, as the spyware could reinstall itself.

Enabling firewalls and installing an anti-spyware/antivirus software, and keeping the software up-to-date, can help detect and remove spyware, but even the best anti-spyware software is not always effective. A reputable and free antivirus program for both PC and Mac is Avast (www.avast.com). Clearing your browser history and deleting cookies will not remove spyware.