Called to Peace

MINISTRIES

**Compiled by Peter Escue**

Cybersecurity Professional

CTPM Church Partner Liaison

Called to Peace
MINISTRIES

# Combatting Technology-enabled Abuse

## Table of Contents

## Introduction

Technology is a core part of our day-to-day lives as we use our cell phones for email and messaging, GPS directions, banking, and many other activities. However, this same technology can be used against victims of DA and understanding some of the ways this happens can help advocates advise their clients of the possibilities.

Making technology secure can be tricky because things are constantly changing. Those changes can be good, but they also introduce new ways that perpetrators can victimize others.

It is unlikely that one perpetrator will use all these tactics, and some of these tactics are fairly unlikely to happen. But they do happen, and the more you know, the better you can prepare your client.

**IMPORTANT:** Be cautious making changes to a victim/survivor's phone because those changes may alert the perpetrator that something is going on. If he is monitoring the phone, he may realize that it fell off the grid for a period of time when, for example, you use a Faraday bag or that the Echo smart device has been turned off. The victim can claim ignorance in those situations, but it's good to be prepared with a story beforehand. You may want to make sure the victim/survivor is safe before making any changes.

## What to do first?

1. If possible, get a new cell phone, with a new number, on a new plan. He may have put spyware on the current phone to track the survivor. Even if he hasn't, he can cause problems if he has a phone on the same account plan as the survivor.
    a. Use this new phone to communicate to friends and family and helpers, not with him, and hide its existence from him.
2. If she has an iPhone, change her Apple ID/iCloud/iTunes password (just different names for the same thing).
3. Set auto-lock on the phone with a PIN or password he won't guess.
4. Create a new email account, without his knowledge.
    a. Gmail is free and convenient, but ProtonMail and Tutanota are secure email providers with free plans. Using one of those might throw him off.
5. Install a messaging app called Telegram on her phone in order to communicate with her counselor and advocate.
    a. When sending a message, make sure to use the "Secret Chat" feature as that can automatically delete messages.

   b. Be careful about trusting WhatsApp or other “encrypted” messaging apps. Many spy apps can read WhatsApp messages.

6. Try not to use any computer or device that he has access to for communications to an advocate, counselor, or lawyer.
7. If you’re sure he’s tracking the survivor via her phone AND you can’t find the spy app, consider one of these options:
   a. Reset the phone to defaults.
   b. Do NOT restore the phone’s apps from the cloud, because you will just restore the spy app. Manually go to the App Store and install them. It’s a pain, but that is the only way to know you’ve gotten rid of the spyware.
   c. Again, consider purchasing a pay-as-you-go phone and keep it in a safe place for private calls. Use a password on your phone and update it regularly.
8. Don’t talk around an Amazon Alexa device. Conversations can be recorded and tracked.

***<u>Remember</u>:***

- ➢ Computer and cell phone use can be monitored without the user’s knowledge.
  - o Computers store information about the websites you visit. That means bills you pay and purchases you make are tracked, and messages or emails can be retrieved. Always consider that a computer might be monitored when you use it and be careful with what you send others or post.
- ➢ When using a web browser on a device he may have access to, try to use it in Incognito mode (for Chrome) or Private Mode (for Firefox or InPrivate Session (for Microsoft Edge).
  - o For Chrome, click the 3 dots in the top right and select “New incognito window”
  - o For Firefox, click the 3 horizontal lines in the top right and select “New Private Window”
  - o For Microsoft Edge, click the 3 dots in the top right and select “New InPrivate window”
- ➢ You can also delete your browsing history, which is a record of all the websites that have been visited.
  - o Click the 3 dots or horizontal lines, and then:
    - ▪ For Chrome, select More tools – Clear browsing history
    - ▪ For Firefox, select Options – Privacy & Security, and then under History click the Clear History button.
    - ▪ For Microsoft Edge, select Settings – Privacy, search, and services – Clear browsing history.

- If she can get out, computers can be found at the local library, Internet cafe, shelter, workplace, or computer technology center. However, since these are public computers they still cannot be trusted completely as they may have malware from other sources.
- Be sure she signs out of her email and other accounts when she is done using them, so he doesn't have easy access to her communications.
  - She should use several different methods of communication when contacting people in order to have backup methods when one method is compromised.
  - Keep the monitored account active with non-critical emails in order to maintain appearances.
- Global Positioning System (GPS) trackers can be placed in or on her car, or on items like her purse or cell phone.

## General Cybersecurity Guidelines

These are general guidelines for computer safety, but perpetrators can use these vulnerabilities to continue to abuse their victims.

- Don't click on a link in an email or text unless it is from a source you trust AND you are expecting it. It is better to search for the website on Google or type in the link yourself in a web browser.
- Don't open any email or message attachments unless it is from a source you trust AND you are expecting the file. Malware and viruses often hide in these attachments.
- Make sure you stay current with software updates for all your devices and apps. Enable Auto-updates on your devices and apps.
- Try to use strong passwords that are unique to each account/site you use. Try not to reuse passwords across accounts.
- Use multi-factor authentication (MFA) if you can.
- Never give out your password over the phone.
- Posts on social media are never truly private, no matter your settings: once it's online, it's no longer under your control. Be protective of your personal information and remember that phone numbers, addresses, handles, and personal details (like birth date, schools you attended, employers, and photos with landmarks) may make it easier for someone to reach you.
- Set boundaries and limits, and ask people not to post personal information, photos, or check-ins you aren't comfortable with. Check your social media settings to make sure your privacy settings are strict and disable the ability for other people to tag you in their photos or posts. Similarly,

don't post information about people without their consent – you could jeopardize their safety or the safety of others.

## Cell Phone Safety

We rely on our cell phones to help run our lives, but they can become a weapon in the hands of perpetrators if we don't treat them carefully.

- Put a passcode on your phone to make harder for someone to get into it.
- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.
- Do not respond to any questions, especially those that can be answered with "Yes" or "No." The caller can record your voice, and then play it back later for nefarious purposes.
- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. There are many services and apps that can spoof phone numbers and names.
- Use caution if you are being pressured for information immediately.
- If you have a voice mail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.

## Device Safety

Computers, laptops, and tablets need strong security also.

- Put a password on your computer or laptop.
- Avoid clicking on links or opening attachments sent to you by someone you don't know or someone you think might want to monitor your computer activity.
- Run anti-virus and anti-spyware software on your computer, and make sure that it automatically updates so you have the latest protection.

- In some cases, you might have to share documents with the person you are concerned is trying to monitor you. Consider using online sharing platforms, such as Google Docs, Dropbox, or Flickr, to exchange information rather than having it come directly into your email.
- Be cautious when using a computer that is not yours. Log out of accounts, erase your activity from the web browser, and don't save personal items onto that computer. If you must save something to the computer, delete it, including from the trash.

## Passwords

The average Internet user has dozens of accounts across dozens of websites, and while password management can be difficult, it is very important to be careful with passwords. A perpetrator can cause a lot of damage if he can figure out how to log in to one of her accounts.

- The length of a password is more important than its complexity. Consider using the name of a favorite song; don't use kids' names or birthdates or something he could guess. Try to use a password that is at least 10 characters long.
- Try to use passwords that are unique to each site. For example, don't reuse the password you use for banking to be your email password also.
- Try not to write down passwords, especially in a place he could find. Assume he is going through her belongings when she is not there and that he is snooping around. He may get suspicious and that will increase the intensity of his searches.
- However, if she can't remember your passwords and need to record them, it is better to physically write them down than to store them electronically on a phone. Or worse, keep forgetting the passwords and resetting them.
- Consider using a password manager like LastPass or 1Password. Don't save passwords in your browser.

## How to determine if you are being tracked via your phone?

1. Check the phone bill for extra large data usage.
2. Has he had access to her phone in order to install a spy app, or does he know her iCloud password?
3. Have any odd messages popped up on her phone screen?
4. Does the phone's battery seem to be draining quickly?
5. Does her phone sometimes turn on for no reason?

6. Are other apps running slower than normal?
7. Does it take forever to shut down?
8. Are there unfamiliar apps running in the background?
9. Does the screen stay on when she tries to turn it off?
10. Check the Permissions of all apps. Permissions include “Call logs”, “Microphone”, “Location”, “SMS”. Try to find any apps that have all these permissions, and then determine if they’re suspicious.
    a. On Android, it is in Settings – Privacy – Permission manager.
11. Does he know things about her – things you’ve said/emailed/messaged – that he shouldn’t have known?
12. On iPhones, enable the App Privacy Report (Settings – Privacy & Security – App Privacy Report. Over the course of a couple of days, this will show which apps are active. You may see one that is unfamiliar.
13. Also on iOS 16+ there is a feature called Safety Check (Settings – Privacy & Security – Safety Check – Manage Sharing & Access) which can help identify who else can see the information stored on this phone. Look carefully who and what apps can access information.

## Miscellaneous Tactics

1. Tracking
    a. There are new devices that are intended to help you find your keys, but they can also be used to track people. Tile (tileapp.com) is a small device that is supposed to be put on your keychain, for example, but can also be slipped into a diaper bag or into a car trunk. Apple has the Airtag, which is used the same way, but will be much easier to track than even Tile.
2. Fake phone calls
    a. There are services where a person can text, and then the service performs automated calls to a list of phone numbers. This can be a useful, legitimate service, but can also be used by a perpetrator to make untraceable phone calls. A perpetrator can, for instance, use the service to mimic the courthouse, calling to supposedly notify a victim of a court hearing reschedule. One of these services is ClickSend.
3. Spoofed Phone Numbers
    a. As most people know, there are plenty of telemarketing firms that can call your phone where Caller ID shows a local phone number. There are plenty of services that can do this for individuals, so a perpetrator can use a service like this to hide his phone number

to get around protective orders. It can be challenging to uncover the real number and may involve multiple phone calls to your service provider and law enforcement. Some services can even change the caller's voice. Some of these services are Spooftel, Spoofcard, and the Bluff My Call app.

4. Smart Home Devices
    a. Smart Home devices like Amazon Echo (Alexa) and Google Nest can be useful but can also be used to listen in on conversations. If a perpetrator can log in to an account where the device is registered, he can turn on a device in listening mode without any notification to the people nearby. Also, he can look to see what else has been done with the device/account, giving him new opportunities to harass his victim.
5. IOT Devices
    a. Other in-home devices that are connected to the Internet can also be used against victims if the perpetrator can access the accounts that control them. Connected lightbulbs can be turned off and on. Nest thermostats can be lowered or raised, whatever would cause the most problems. Refrigerators, robot vacuums, connected cars, music speakers, baby monitors and security cameras are all susceptible to abuse. Either change the account passwords so the perpetrator can't access them or get rid of the devices.
6. Same Cell Phone Plan / Apple Account
    a. If the victim/survivor's phone is on the same account as the perpetrator, he may be able to track the victim as well as play games with the phone's service. He can, at will, turn off and on service to the phone, causing confusion and potentially significant problems when the victim misses important calls. Also, being on the same Apple account may allow him to see what applications the victim is installing. If she installs, for instance, Telegram, he may have the account set up where the same app gets installed on his device too. Be careful how you proceed with her phone so as to not alert him while she is still in danger. It is better for her to get a new phone on a new plan.

## Ways to Counter Harassment

- If your texting or messenger service allows you to create a username, consider using a name that doesn't identify who you are.
- Use a virtual phone number, such as Google Voice (https://voice.google.com), which is an alternative phone number that you can use to send and receive phone calls and text messages.

- Document the harassing email and don't delete it. While it may be tempting to delete the message, some of the best evidence is in the full header of the original email. It is sometimes possible for emails to be traced back to the sender, even if she or he is using a fake email address.
- Use a Faraday Bags to disconnect your phone completely. Named after a physicist, a Faraday bag or box can be used to isolate a cell phone from all electrical signals. By putting a cell phone in a Faraday bag or box, it is cut off from all signals including cellular, WiFi, and Bluetooth. You might want to put a client’s phone or device in a Faraday bag while you talk to ensure that the perpetrator can’t eavesdrop. Using this might be necessary when the victim is not sure if the perpetrator has compromised the cell phone with spyware or is tracking the cell phone. However, if the phone drops off the grid, the perpetrator will know something is up, so be careful how you use it. Here is an example of a Faraday bag for a phone: https://www.amazon.com/gp/product/B01A7MACL2/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1
- If you don’t want to continue to see the harassing emails (but may not want to shut down the account so you can continue gathering evidence) you could open a new email account, one that the person harassing you doesn't know about.
- In some circumstances, you might need to communicate with the other person. Create an email account specifically for that communication. For additional security, check that email from only one specific device. This way, if the other person should manage to successfully send spyware or malware, it will affect only that device.
- Have more than one email address and use them for different purposes. If you must communicate with someone who is harassing you, limit all interaction to just one email address.
- Always run anti-virus and anti-spyware on your computer or laptop to protect your device. A good example of a free anti-virus package is Avira.
- Use strong passwords for your email accounts.
- Go through your online accounts' privacy and security settings. Privacy settings can be used to limit who can see your content. Security settings control access to your account.
- Many social media websites ask for a lot of personal information. Share only what you’re comfortable sharing and use privacy settings to control who can see what.
- Don’t feel pressured to be friends with people you don’t know or want to know. It is your social media space and you choose who to include in that circle.
- If you have a high privacy risk, consider limiting what you share. Social media is inherently a public space.

- If the site allows it, use a pseudonym to protect your identity.

## Impersonation

- Search for your name or nickname on various social media sites to see if accounts pretending to be you have been created. If you find them, report them as fake accounts.
- If you get a friend request from someone with whom you're already friends, ask your friend if she or he created a new profile. If not, it could be someone else who created the profile pretending to be her or him.
- Use 2-step verification, which requires a secondary password when your account is accessed from an unknown device or location.
- Use a strong password that other people can't guess. Try not to use the same password for all of your accounts.
- Some sites allow you to reset your password by answering secret questions. Because the answers to these secret questions are often known by other people (your first car, for example), you don't have to answer these questions honestly; you just need to know what your answer was if you need to reset your password.
- Make a list of all of your accounts so that if you do need to update passwords, you know all the accounts you have.

## Helpful Resources

Here is a list of potentially useful apps, from recording conversations and phone calls to keeping a log of abusive incidents to how to recognize an abuser.  Some of these cost money, and all should come with your guidance, so be sure to review these before recommending them to a client.

- Record conversations
  - Voice Memos (on iPhones)
  - Rev Voice Recorder and Memos (or any Voice Recorder app)
  - TapeaCall Pro (for phone calls)
    - These apps can be useful to record conversations for later playback; make sure it is legal in your state to record a conversation without the other person’s permissions BEFORE you do it
- Automated Danger Assessment and Help
  - myPlan
  - RUSafe

- Personal Safety App
    - Noonlight
- Document Incidents and Evidence Collection
    - DocuSAFE
    - Websites
        - Document the Abuse (documenttheabuse.com)
        - VictimsVoice (https://victimsvoice.app/)
- Technology Advice
    - Tech Safety app
        - https://techsafetyapp.org/
    - Organizations
        - Operation Safe Escape
            - https://safeescape.org/
        - Ohanalink Purple
            - https://www.ohanalink.com/purple
        - Safety Net Project
            - https://www.techsafety.org/
        - Clinic to End Tech Abuse (CETA)
            - https://www.ceta.tech.cornell.edu/
        - Coalition Against Stalkerware
            - https://stopstalkerware.org/