

## Introduction





This document identifies the most common tech safety issues that clients describe to us. Each issue is paired with a checklist of potential indicators of concerns, common causes roughly ordered by likelihood, and solutions.

There is redundancy in many of these checklists, as a single point of compromise can manifest in multiple different ways. **It is intended as a quick reference for volunteers to map client concerns to potential remedies.**

**These lists are not intended to be, nor can they ever be comprehensive.** If you are in doubt as to whether or not you've missed a potential avenue of attack or if you run into an unfamiliar issue, *always* consult with the Slack channels #clinic-practice and #techsafety. It is never too late to send follow up information, and remember, we are not an emergency service!

It also links to, but does not replace, the existing step-by-step guides used to walk through a solution. Please always consult the guides for a full walkthrough, including warnings about visibility to abusers and evidence documentation.

## Legend

-  Course of action may be visible to the abuser. Notify client.
-  Evidence documentation checkpoint. Remind client to take screenshots.
-  Probe the client for more information.
-  Hypervigilance indicator.

## Table of Contents:

- [General](#)
- [Location Tracking](#)
- [iCloud/Email Monitoring/Tampering](#)
- [Text Messages Monitoring/Tampering](#)
- [Phone Conversation Monitoring](#)
- [Harassment \(social media + phone calls\)](#)
- [WiFi and Network Compromise](#)
- [SIM swapping and cloning](#)
- [Video/Audio Recording Devices](#)

## General

It is not uncommon for clients to omit details that provide helpful clues without additional probing. Particularly relevant probing prompts are noted in each section. However, it is always a good idea to prompt the client with the following questions:

- Do you worry that your device(s) is being used to track you?
- Does the abuser show up unexpectedly or know things they shouldn't know?
- What devices do you use in your home or carry with you? (e.g., smartphone, iPad, baby monitor, tablet, desktop, laptop, kindle, echo, etc.)
  - Do you currently (or have you in the past) share(d) your devices with your abuser?
  - Is there any chance that your abuser has (or had) physical access to your devices?
  - Do you share a phone/Internet plan with the abuser?
- If abuser is a former spouse/partner, do you share custody of any children who may have devices?

[\[top\]](#)







## Location Tracking



If an abuser can track a survivor's real-time location via spyware or a dual use app, they may show up in person and harass or harm them. Alternatively, knowing a survivor's agenda (e.g. an e-calendar) is enough to know where they will be at what time. Knowing where a survivor has been in the past — for example because they are able to see where payments have been made — can be used by an abuser to intimidate or stalk a survivor.

### Client Indicators

- The abuser always or sometimes seems to know where the client is
- The abuser is using information about the client's whereabouts in legal proceedings (e.g. child custody)
- The abuser explicitly states they are tracking the client
- Client has general safety concerns and would like to check overall safety

### Possible Causes + Actions

- **[If iPhone]** Location settings on iCloud.
  - Check iCloud location settings including FindMy.  
  - Check family sharing settings  
  - [Check iCloud security.](#)
- **[All devices]** Location settings on Google Account (Google Maps)  

- Possible unidentified tracking device 
  - **[If Android]** Apple app to scan for AirTags on Android: **AirGuard or Tracker Detect**
    - **Note that Tracker Detect is notably difficult to use.**
    - Check devices in bluetooth + WiFi range (for e.g. Tile or other trackers)
- If location tracking seems limited to vehicle, OBD ports, SmartCar apps, or built-in tracking for registered owner of car can be checked by mechanic.
- Child devices and trackers in child items if shared custody
  - in particular tablets (e.g. Kindle Fire), smartphones, laptops, and trackers
- Abuser may have proximal (indirect) info about client's location via access to text messages/calendar or financial accounts (e.g. credit card logs or receipts indicating location) with details about client's schedules or travel history.
  - Refer to sections on [text message](#), [Gmail/email](#) access and [financials](#).
  - **? Probe:** Ask about client's social media usage and whether location information might be shared on social media (including geotags).
- **? Probe:** Does the client have any devices they haven't mentioned?
- [All devices] **? Probe:** Has the abuser had physical access to the device? Does the client still have physical contact with the abuser?
  - If yes, **high risk** for spyware/dual-use app. Check apps with location access. 


## iCloud Monitoring/Tampering



For clients with iPhones or Apple devices, an abuser who has access to an iCloud can access a host of information such as location data, Notes app, photos, text messages and iMessages, voicemail. This is a standard safety check for any client with an Apple device and should almost always be performed if applicable.

### Client Indicators

- Client has iPhone or Apple device (always a good check)
- Abuser can access information stored in a wide array of applications installed on iPhone or Apple computer, such as Notes app, photos
- Text messages and/or e-mails are disappearing or mysteriously marked as read
- Client has general concerns about online safety and wants holistic check up

### Possible Causes + Actions

- Check for suspicious log-ins in iCloud 

- If not currently logged in, may be signing in and out. 2FA + password change and/or suggest that client use a password manager.
- **! Check email ([Gmail](#) or [other email](#)) used as AppleID**
  - **!** Check recovery email and recovery phone numbers and do this **recursively** e.g. check recovery accounts for the recovery account.
- Check location settings  
  - See location check for iPhone above
  - FindMy + apps with location access
- Check for old devices used by client that were given to abuser
- Ask about shared phone plan

[\[top\]](#)










## Gmail/Google Account Monitoring/Tampering





Gmail accounts are linked to Google accounts. We distinguish Gmail (and their associated Google accounts) from other email providers. Access to a Google account discloses far more information (e.g. real-time location) than other emails, and may also be linked to an Android phone.

### Client Indicators

- Client has a Google account, Android, or Gmail (always a good check)
- Emails or texts in messaging app are disappearing, mysteriously marked as read
- Abuser seems to see or have access to photos
- Abuser has location access
- Client has general concerns about online safety and wants holistic check up

### Possible Causes + Actions

- Check for suspicious log-ins in Google Account 
  - If not currently logged in, may be signing in and out. 2FA suggestion.
- Check Google accounts linked to Android phone (guide)  
- **!** Check recovery email and recovery phone numbers  
  - **!** recursively check recovery accounts!
- Check location sharing settings (Family + Sharing Tab)  
- Google Family Link settings  

- default system app but need to check if abuser is added
-  **Probe:** Ask about old devices used by client that were given to abuser
- Check email forwarding and shared email settings  
- Is client on shared Internet plan? Are they the account owner? 
  - Won't give direct access to email but may explain some "web monitoring" behavior if abuser can access Internet history
- If interested in offering Norton LifeLock, it is only beneficial for Android phones

[\[top\]](#)










## Email Monitoring/Tampering

Email access not only grants the abuser visibility into sensitive or personal information in the emails themselves, but can also be the root cause of other harms: email is often used to sign into other online accounts including social media and financials, may be linked to a calendar giving clues as to location, may be a recovery email for an iCloud/Google account, and may impact the client's ability to earn a living if it is a work or business account. While non-Google accounts typically don't directly track location, they can give alarming proximal information or allow access to an account that does.

### Client Indicators

- Client has a non-Gmail account and/or recovery email is not Gmail)
- Emails are disappearing, mysteriously marked as read
- Abuser seems to know content of emails
- Most other emails do not have location access but proximal info such as receipts (indicating travel history) or calendars may be linked to email
- Client has general concerns about online safety and wants holistic check up

### Possible Causes + Actions

- Check for suspicious log-ins. May need to search for email specific guide.  
  - If not currently logged in, may be signing in and out. 2FA suggestion
- Check recovery email and recovery phone numbers  
  -  recursively check recovery accounts!
-  **Probe:** Ask about old devices used by client that were given to abuser
- Check email forwarding and shared email settings  
- Is client on shared Internet plan? Are they the account owner? 
  - Won't give direct access to email but may explain some "web monitoring" behavior if abuser can access Internet history

[\[top\]](#)

## Text Message Monitoring/Tampering

### Client Indicators

- ▲ Not receiving text messages
- Text messages deleted
- Abuser knows content of text messages
- 💡 **Probe:** what text application does client use? iMessage? WhatsApp? SMS ("regular" text messaging)? Facebook's Messenger?

### Possible Causes + Actions

- [iPhone] [Check for iCloud compromise/access](#)
  - Check if iCloud storage is at capacity
  - Check which phone numbers and emails are allowed to send and receive messages associated with this AppleID, including message forwarding
  - Check how long messages are saved for until automatically deleted
- Ask client if using shared phone plan
  - Refer client/caseworker to legal counsel for exit under [NY State Law](#)
- [Android] Google Family Link settings (default system app in Android but need to check if abuser is added to settings)
- Check for suspicious apps that have permission to SMS/text messaging
  - May include default provider apps. Ask about phone service/model.

[\[top\]](#)

## Phone Conversation Monitoring ▲

It's vanishingly rare for abusers to have the technical capacity to listen in on phone conversations. Clients who express concerns about phone conversation monitoring may be experiencing hypervigilance surrounding technology. Nonetheless, we should still treat their concerns with dignity and do due diligence in probing for information and checking for spyware, especially in high-risk cases,

### Client Indicators

- ▲ client reports that abuser knows information spoken about on telephone calls
- client reports or consultant hears beeps, mechanical sounds on phone lines
- ▲ dropped calls/client misses incoming calls that do not show up on log
- abuser claims that they are listening to phone calls and conversations
- ▲ Frequent spam calls

### Possible Causes + Actions


- Check for other evidence of account compromise
  - abuser may be accessing knowledge through other technical means (e.g. text messages, voicemail) or through non-technical (e.g. mutual contacts) means, and claiming that they can "hear phone calls" to scare client
  - Probe for and check [iCloud](#), [text message](#), and [Gmail](#) or [email](#) security
- **? Probe:** Is client on same/shared phone plan?
  - Refer client/caseworker to legal counsel for exit under [NY State Law](#)
- Possibly (and more likely) non-technical means of learning about phone calls, e.g. through shared/mutual contacts or children
- [SIM swapping](#) where the POC took control of the phone number (for a period of time)
- Spyware/malware, especially if other IOCs evident like dropped calls, short battery, phone running hot.
  - **? Probe:** did abuser have physical access to device?
- [V/AR installed in home](#). More likely if client is currently separating from abuser.
  - **? Probe:** did abuser ever have physical access to home?



[\[top\]](#)

## Harassment (social media + phone calls + spoofing)

Harassment usually doesn't need to be diagnosed, as clients know if they're being harassed. It is unfortunately difficult to proactively prevent, especially without limiting the functionality of the client's technology. Setting expectations with client is important. However, here are some potential solutions.

### Possible Solutions

- If abuser is directly contacting client, the client can request order of protection from lawyer
  - note that this is punitive, not preventative. We do not give legal advice but can contact case worker to request legal services (with client permission)
- "Allowlist" by blocking/filtering calls/messages from unknown numbers.
  - only if client does not need to receive phone calls from unknown number (e.g. client not receiving calls for a court case or doctors appointments)
  - Can purposefully delete contact information of harassers to filter them
- Client may set up a Google Voice or other ersatz phone number and distribute it to trusted contacts, in order to help with filtering calls. **Discuss pros/cons.**
- Privacy settings on social media may be set to more conservative level. 

- We can also contact social media sites to help report harassment
- Check if number has been publicly listed on any websites/Google
- Check if Call Forwarding is configured  
- "Code phrases" with trusted contacts to avoid/prevent spoof attacks

[\[top\]](#)

## WiFi and Network Compromise ▲

Suspicion of WiFi and network monitoring is often a catch all for suspicious and may be an indicator of hypervigilance/mistrust in technology. Even if the abuser can access the clients WiFi, there is very little they can do with that access. However, we can and should still recommend common sense measures such as ensuring their WiFi is not private, changing the password, and not visiting suspicious sites or links.

### Client Indicators

- ▲ client reports that abuser can see all their internet traffic
- unusually slow WiFi/Internet, especially across multiple devices
- ▲ client reports abuser has used network in past and fears they still have access

### Possible Causes

- **? Probe:** is the monitored activity specific to one to two potentially compromised accounts? might it be hacked email(s) used for wide access, e.g. as the log in to many accounts? did the abuser inherit any old devices?
- **? Probe:** if client reports slow network, is the network slow across multiple devices?
  - If it is limited to one device, it may be benign (obsolete hardware, uninstalled software/OS updates, full hard disk) or suspicious (spyware/malware).
- **? Probe:** is abuser named on the Internet service account?
  - Refer client/caseworker to legal counsel for exit under [NY State Law](#) (applies to cable accounts as well as phone)
- WiFi scan using router page or Fing app to show devices on network
- Encourage client to change WiFi password to strong password.
  - warn client that this will sign out all of the other (legitimate) client devices on the network so they are not frightened/surprised later.
- **Inform:** useful to let client know that if the client is using their own private network of which they are the sole account holder, even other legitimate devices



cannot see their network traffic on most webpages, including most banks/social networks.

[\[top\]](#)

## SIM Swapping and Cloning

### Client Indicators

- client reports that they lost use of their phone number
- reports that SIM was removed from phone
- POC has had physical access to phone

### Possible Causes

- **Probe:** what did client observe that led them to believe they lost access to phone number?
  - ▲ Temporary service failures (bad signal) are not good evidence of SIM swapping.
  - Received text message from cellular company that the SIM was being changed for the phone number
  - Cellular connectivity bars are X'd or greyed out, cannot make phone calls/texts
  - The above, combined with notifications about account activity (password reset or sign in) on accounts tied to phone number
- **Probe:** did client contact cellular provider?
  - If cellular service confirmed that phone was moved to another SIM as requested by someone (but not the client), then this is possibly a SIM swap.
- **Probe:** did clients obtain access to the phone number again?
  - Still may have happened in past, consider discussing account security
- **Probe:** does client have an online account with cellular provider?
  - Access to account by POC could help enable SIM swap or other cellular monitoring
- **Actions:**
  - Suggest contacting cellular company, regaining control of phone number, asking about and enabling additional protection against SIM swaps. For

example, many allow setting a secret PIN that must be given to change SIM

- Enumerate accounts to which phone number may have given POC access, check their security
- **Inform:**
  - SIM cloning is not feasible for modern SIM cards. Losing use of phone number always happens with SIM swapping.

[\[top\]](#)

## Video/Audio Recording Devices ▲

V/AR is most likely with clients who either live with their abuser or who used to live with their abuser in their current home until recently. It is also especially likely if they share children ("nanny" cams) or have installed their own V/AR devices for safety and security. However, suspicion of V/AR can also be an indicator of hypervigilance.

Detecting V/AR is difficult for us to do, and you should set expectations with the client that we cannot do home scans. However, we can guide the client through some steps to find and/or disable V/AR. **V/AR will usually need both a power source and access to the Internet/Bluetooth in order to transmit any recorded data.** Changing WiFi password can knock off many V/AR devices.

### Client Indicators

- Client has received direct threats from abuser (e.g. "I'm watching you")
  - Abuser may be bluffing or overstating
- Has installed their own V/AR for security but is worried about access
- Experiencing frequent electronic disruptions
- Has documented many instances of spying with no evidence of account/device compromise
- Client shares children with abuser who at some point had physical access to home, especially having recently lived together

### Possible Causes + Actions

- **? Probe:** has abuser had physical access to space? do they still? child devices/mutual contacts?
- **? Probe:** do you have an Amazon Ring or other online camera account?
- However, V/AR requires a power source and usually requires bluetooth WiFi.

- Guide <TODO: link to home sweep guide>

[\[top\]](#)

suspicious or sensitive permissions for remote spyware check:  
location, keyboard, microphone, camera


## Financial Attacks

A client may have loans, credit cards, joint bank accounts, and shared assets with an abuser. A survivor's financial account can contain more than just financial information, such as a mailing address, contact information, location information (transaction meta-data), and more. Most often, financial abusers use technical attacks to monitor a survivor's financial activities (e.g., tracking and monitoring for finances), exploit their financial assets, restrict their access to financial accounts, and sabotage their financial stability. These attacks are difficult to prevent, just like harassment. It is possible to curtail some aspects of financial attacks, however, by enforcing good security and privacy practices.

Other scammers and fraudsters can be responsible for financial attacks, so an abuser might not be responsible. Financial concerns can seem like technical problems (e.g. incorrect credit report information online) but are sadly beyond CETA's scope to resolve. Nevertheless, there **are** some ways we can help! If in doubt, see about sending **Rosie Bellini** (rbellini@cornell.edu) a message on slack or email around anything you are unsure of.

## Client Indicators






- Client has received direct threats from abuser (e.g. "I know how much money you have/make")
  - Abuser may be bluffing or overstating
  - Abuser may have survivor accounts added to a third-party personal finance management app (e.g., Mint, INTUIT)
- Client is receiving emails/receipts about purchases they have not authorized
- Client may have received a push notification from their mobile wallet that their registered card was used.
- Client may have received a security alert from a financial institution about someone attempting to access a bank account.
  - These may be phishing if further information is requested from a client!

- Client sees ‘suspicious’ activity on any financial account (e.g., fraudulent transactions, missing money, new accounts being opened without their knowledge)
  - Encourage client to take evidence 
- Client may have received calls or letters sent to them describing financial products they have no knowledge of.

### Possible Causes

- **? Probe:** has an abuser ever had physical access to your wallet/purse? what about your cards?
- **? Probe:** do you have any shared financial accounts with abuser? have you ever had one in the past? are they still active now (e.g., not closed)?
- **? Probe:** are you an authorized user on abuser’s accounts (i.e. can you use any of their cards)? is the abuser an authorized user on any of your accounts?
- **? Probe:** do you use a browser-based password manager? a standalone password manager? do you store financial information there?
- **? Probe:** does abuser know about all of your financial history or just some of it?
- **? Probe:** is any of this financial information already available online? (e.g., on open business pages)

### Actions

- Check for evidence of account compromise; each financial service will have a ‘Security Center’ which gives a breakdown of connected devices + logins 
- Encourage client to change account username and password 
  - This will sign an abuser out of any shared devices
  - Changes to log in information will also uncouple any personal financial management app accounts too (e.g., INIUIT mint, yolt etc.)
- Encourage client to change answers to security questions 
  - If all answers to a security question are known, enter a mismatched pairing of question to answer. “E.g. What was your first model of car?”  
“Answer: Portland” (The answer to “Where were you born?”)
- Turn on an additional stage of security for financial accounts (e.g., 2FA, required branch visit) 
  - Warn client this may sign an abuser out of any shared devices
- Encourage client to remove an abuser numbers from any monitoring alerts 
  - Alternatively, setting up credit alerts via Experian/CreditKarma to a secure email address could alert a survivor to changes in their credit.

[\[top\]](#)