Hey Siri! How do you Increase Accountability and Safety in Stalking Cases?

This project was supported by Grant No.15JOVW-23-GK-05162-HARA and 2020-TA-AX-K033 and awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

LETTAC

SPARC

Objectives

- Identify strategies to investigate cases involving digital evidence when there is no access to a forensic investigator
- Define safety strategies for victims in cases involving technology-facilitated abuse
- Illustrate ways for law enforcement and advocates to collaborate to increase safety and accountability in technology-facilitated abuse cases.

Tech-Facilitated Stalking

LETTAC

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

SURVEILLANCE

- Smart home devices
- Tracking software/GPS
- Cameras/recordings
- Monitoring activity online
- Access to accounts

LIFE INVASION

- Unwanted contact online, texts, calls
- Impersonating victim
- Hacking victim accounts

INTERFERENCE

- Posting private photos or info
- Spreading rumors
- Doxing, swatting
- Controlling accounts
- Posing as victim and creating harm

INTIMIDATION

- Blackmail
- Sextortion
- Threats - release false private info
- Threats - interfere with property, employment, other
- Threats - harm online

Mechanisms of TFS

they OWN something

- Abuser owns device/account
- Shared account/device
- Buying or gifting the survivor the devices

they ACCESS something

- Physical/coerced access to unlocked device
- Remotely "hack" via security questions/passwords
- Install spyware/ "dual-use" app

they CONTACT someone

- Call/text/message victim or friends/family
- Post harmful content publicly (.e.g, threaten violence)
- Proxy harassment
- "Spoofing"

they SHARE something

- Blackmail by threat of exposure
- "Doxxing" victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

TFV: Stalkers can cause harm if...

they OWN something

- Abuser owns device/account
- Shared account/device
- Buying or gifting the survivor the devices

they ACCESS something

- Physical/coerced access to unlocked device
- Remotely "hack" via security questions/passwords
- Install spyware/ "dual-use" app

ADVOCACY

they CONTACT someone

- Call/text/message victim or friends/family
- Post harmful content publicly (.e.g, threaten violence)
- Proxy harassment
- "Spoofing"

they SHARE something

- Blackmail by threat of exposure
- "Doxxing" victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

TFV: Stalkers can cause harm if...

they OWN something

- Abuser owns device/account
- Shared account/device
- Buying or gifting the survivor the devices

they ACCESS something

- Physical/coerced access to unlocked device
- Remotely "hack" via security questions/passwords
- Install spyware/ "dual-use" app

they CONTACT someone

- Call/text/message victim or friends/family
- Post harmful content publicly (.e.g, threaten violence)
- Proxy harassment
- "Spoofing"

they SHARE something

- Blackmail by threat of exposure
- "Doxxing" victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

LAW ENFORCEMENT

Unique Features of TFS

Old stalking, new methods -- and some unique features:

- Extend reach over time and space
  - Reach intimate spaces, resurface after years, more opportunities

- Less accountability
  - Anonymity, seen as "less serious," often thwarts existing protections
- Crowdsourcing attacks
- Entrench existing inequities
  - Safety features and resources are typically resource-gated

Simple Methods, Big Harm

Stalkers often overstate their abilities with technology as a form of manipulation

- Most TFS makes use of simple tools, like third-party apps or social media
- These simple methods can be very powerful, especially when they circumvent normal protections

But simple methods can also stop stalking

Strategies for Investigations

- Identify and comprehensively document stalking behaviors
- Effectively document and capture the victim's feelings, experience, and understanding of what has occurred
- Present options to bring the victim in for a follow-up interview
- Identify what the victim has and what is needed
- Involve advocates as early in the investigation as possible
- Identify when you will need tech or additional support

How Can I Use Electronic Evidence? Stay Offender-Focused

- Illustrate offender's manipulative behavior
- Focus on offender's prior bad acts to show intent, absence of mistake or accident or attitude toward victim (404(b) evidence)
- Highlight power differences between offender and victim
- Rebut offender's claims (victim seeks revenge, is lying, etc.)
- Demonstrate prior consistent statements
- Explain counterintuitive behavior (failure to report, returning to offender)

Questions for Survivors: Ownership

- Who typically bought or set up the survivor's tech?
  - Did the stalker buy/gift the survivor watches, headphones?
- Who pays for the survivor's phone services? Who is the account holder?
- Are there children involved who have electronic devices?
  - Who bought and set those up?
  - Is there a custody arrangement in play?
- Did the survivor leave behind phones, tablets, computers?
  - What did they use those devices for? Checking email or accessing sensitive accounts?

Questions about Access

Did the stalker...

...make the survivor show them their phone, online messages, emails?

...ask or coerce them to share passwords or unlock codes?

...seem like they knew the content of the survivor's messages?

...have a history of stalking/seem to know the survivor's location too well?

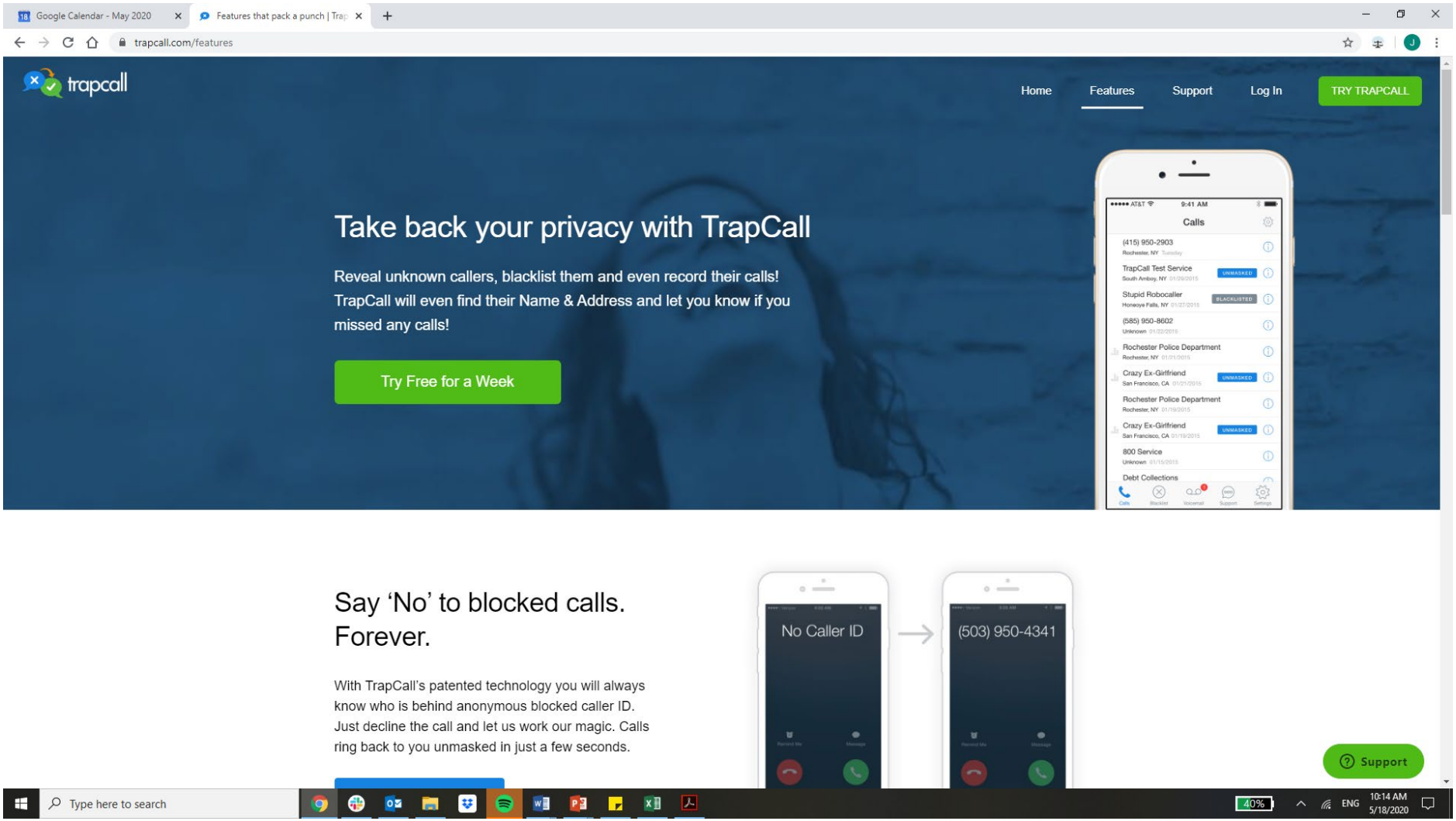
...have access to children's devices?

Unidentified Caller

LETTAC

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

*67 Calls: TrapCall (trapcall.com)



Documenting Anonymous Calls

TrapCall - paid app that reveals the caller ID of blocked numbers. Other services: MaskOff, BaseCaller–YMMV

NumLookup - a free service at www.numlookup.com that will pull callerID as well as **subscriber platform** (e.g. AT&T, TextNow, Google Voice)

#NumLookup

Text Now and App-Based Communication

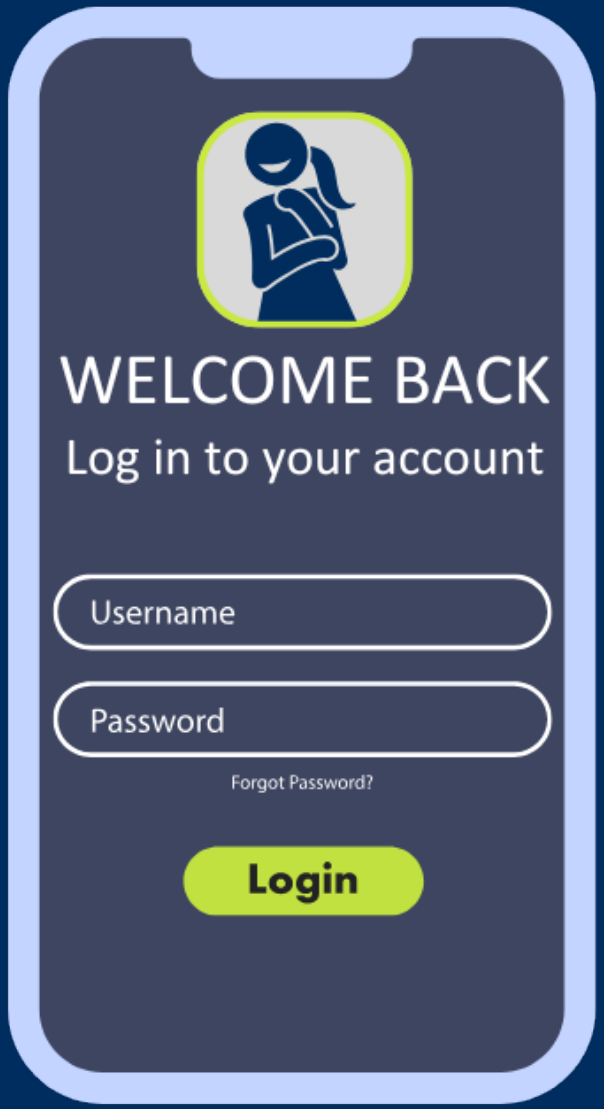
- We get a lot of *Text Now* or app-based phone calls and texts
  - *Using Freecarrierlookup.com
  - *Search.org
  - *Context of the message
  - *Is there a significance of the calls?
  - *Screenshots are important!

Act Fast!

- Subpoena/court record/search warrant for…
  - Victims phone
  - Suspect's phone
  - Financial records
  - The company themselves

Two Components to Phone Security

- Compromise of the device itself
  - Fixed by getting a new device or factory reset
- Compromise of accounts on the device
  - Persists across new devices or reset, needs manual review
  - “Chases" the survivor across devices



Shared Phone Plans

Whoever owns a phone plan can:

- view phone numbers called or texted (but not content)
- fully take over and/or disconnect the victim's phone number
- if set up correctly, turn on location tracking

Date	Time	To	From	Direction	Message type
03/27/2025	06:48 PM	408-2	701-	Received	Picture/Video
27/2025	01:40 PM	408-2	866-8	Received	Text
03/26/2025	08:51 PM	408-204-3	877-2	Received	Picture/Video
03/26/2025	06:08 PM	408-2	562-	Received	Picture/Video
03/26/2025	05:00 PM	408-	743	Received	Text

Safe Connections Act

- Safe Connections Act: a federal law granting a victim the right to leave a phone plan without fees, charges, knowing the PIN, or alerting the owner.
  - Must provide written attestation from a support worker or copy of a police report or restraining order to attest to DV status.
  - Most phone companies have dedicated customer service to this: e.g. https://www.verizon.com/support/domestic-violence/

Securing a Phone: Account Issues

Log in

Passwords or log in methods are not safe

Sharing

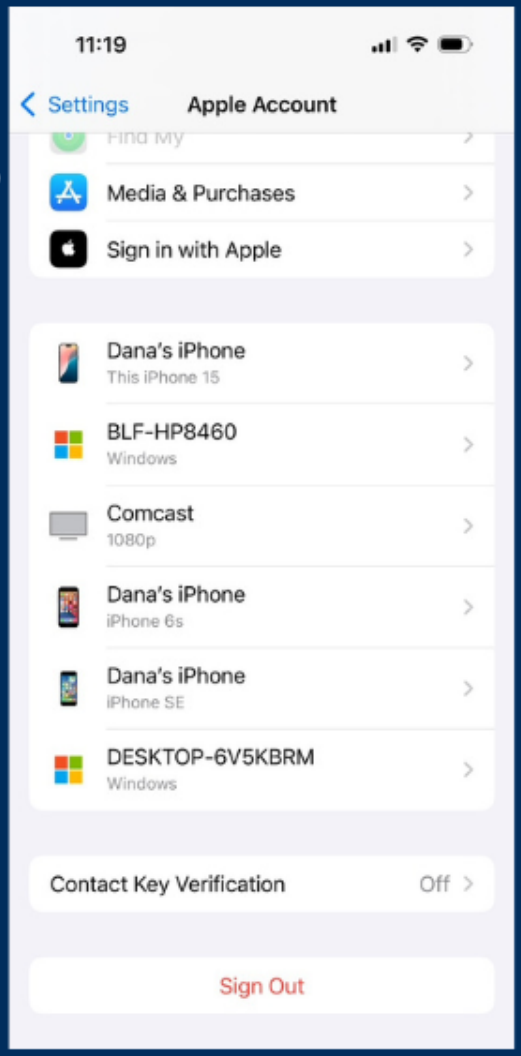
Settings to “share,” such as “Share Location,” are unsecure

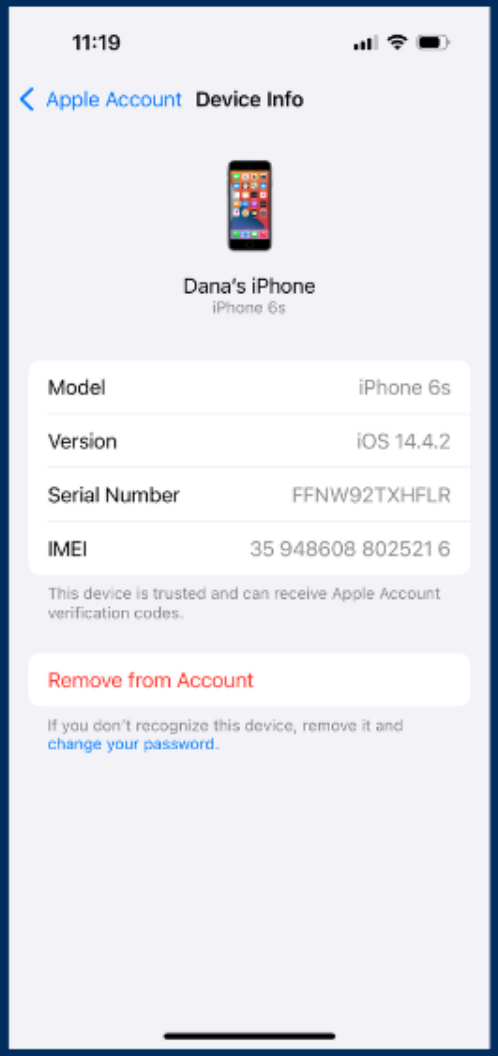
Apps

Apps on the device are shared or use an unsecure login

Account Safety: Secure Logins

- Important online accounts include e-mail, social media, messaging, financial, e-commerce
- Check for unknown log-ins - and document and then remove unfamiliar devices
  - Usually in Settings
  - Is there another phone, laptop, etc. logged into the client's email, iCloud?
    - Would it be safe to remove it?
    - Should we document that access?



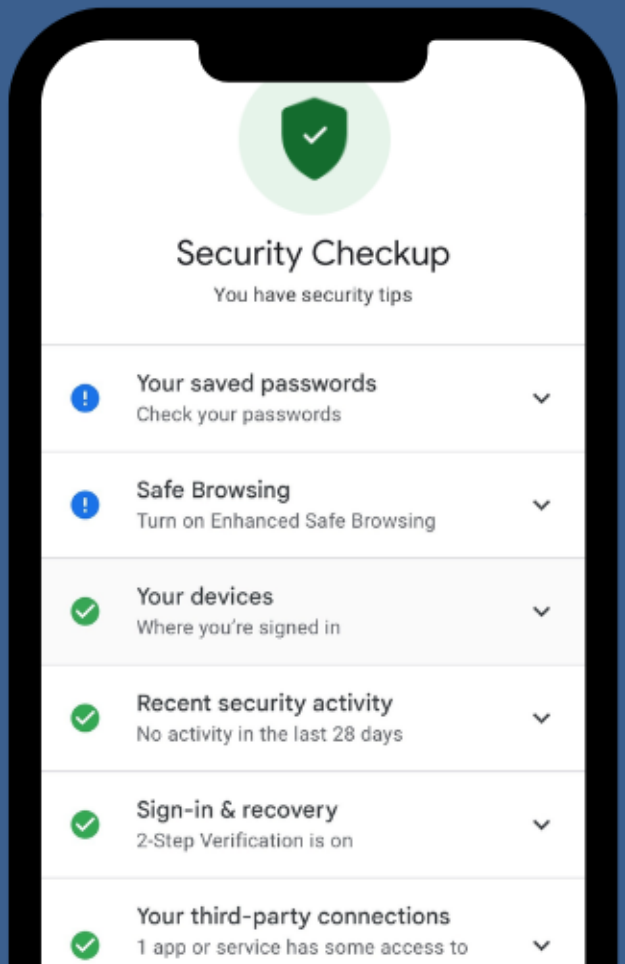


Account Safety: Secure Logins

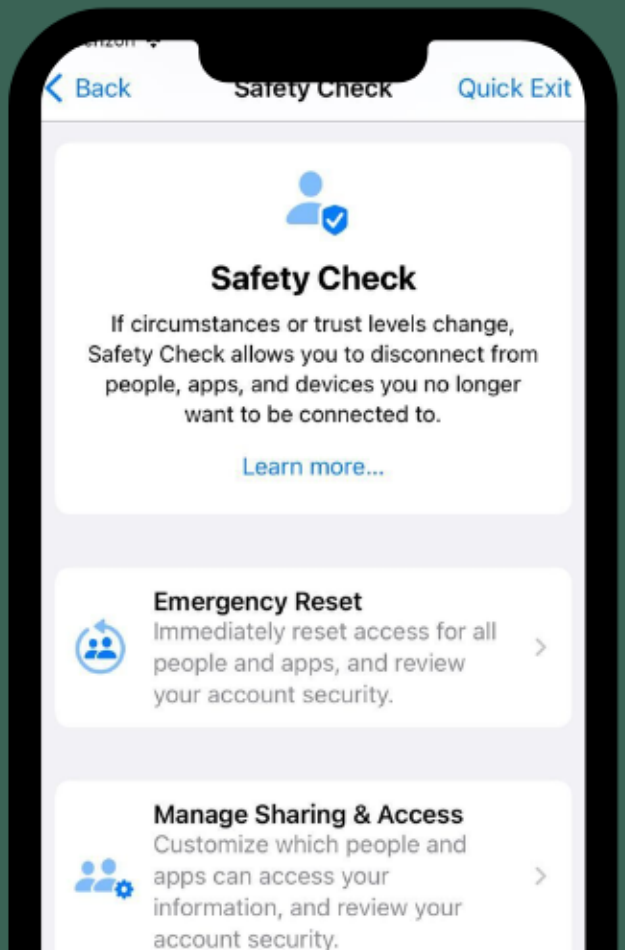
Changing passwords to accounts goes a long way

- Strong passwords are <u>not</u> based on personal information
  - No favorite sports teams, pets, birthdays
  - Use a random combination of letters and numbers
  - Write it down somewhere safe or use a password manager
- Classic security question answers are not resistant to stalking
  - Stalkers may already know or can learn information like the victim's mother's maiden name, first car, city where born
- Be realistic! A password manager isn't right for everyone
- Use 2 Factor Authentication

Android and Gmail users should use Google's Security Checkup



Apple users should update their phones and use Apple's Safety Check



Always Do a Gmail Safety Check

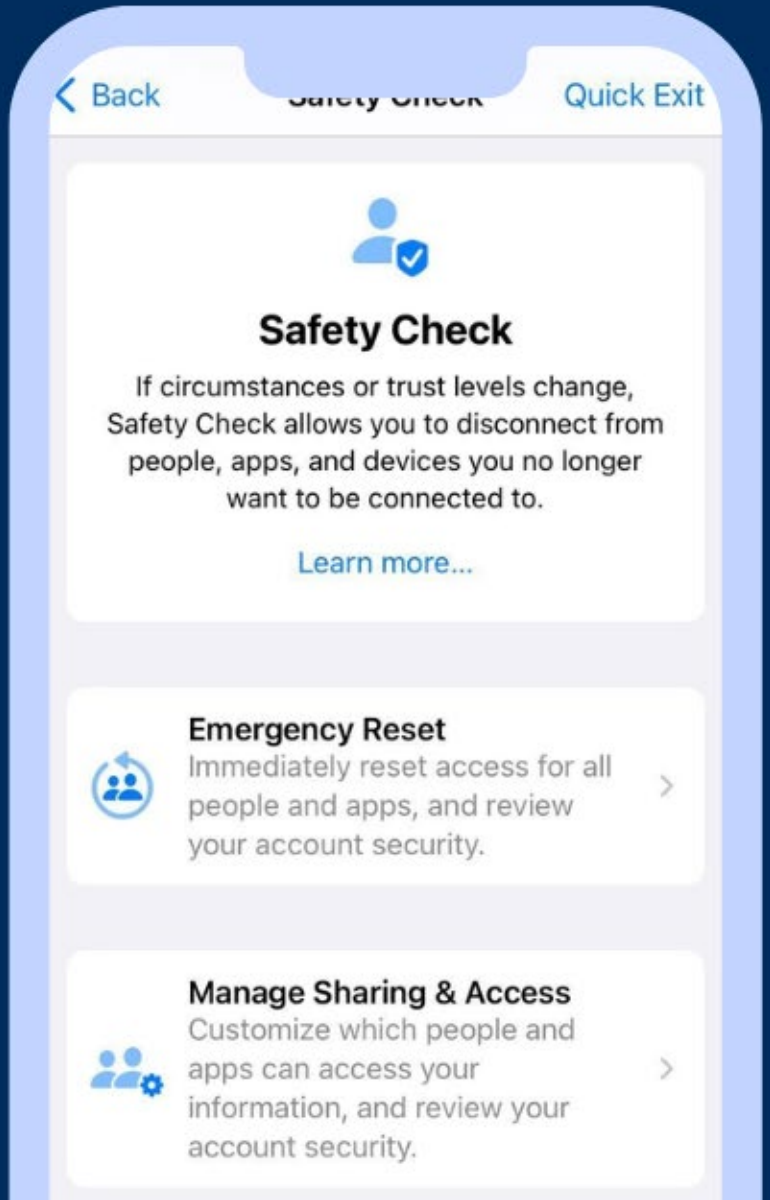
A Gmail account is connected to and controls the key safety elements of an Android phone! A Gmail account is also the key to MANY other important accounts for password reset.

- Go to https://myaccount.google.com/security-checkup
  - Review all tabs, including location tracking and signed in devices
  - Or type "Safety Checkup" into google and go to checkup

- Check access, sign-in, recovery, and sharing - including email forwarding or linked accounts

Apple Safety Check

- Where?
  - Settings > Privacy and Security > Safety Check
- Why?
  - Location tracking, text messages, phone call history, e-mails, credit cards
  - Highest risk!



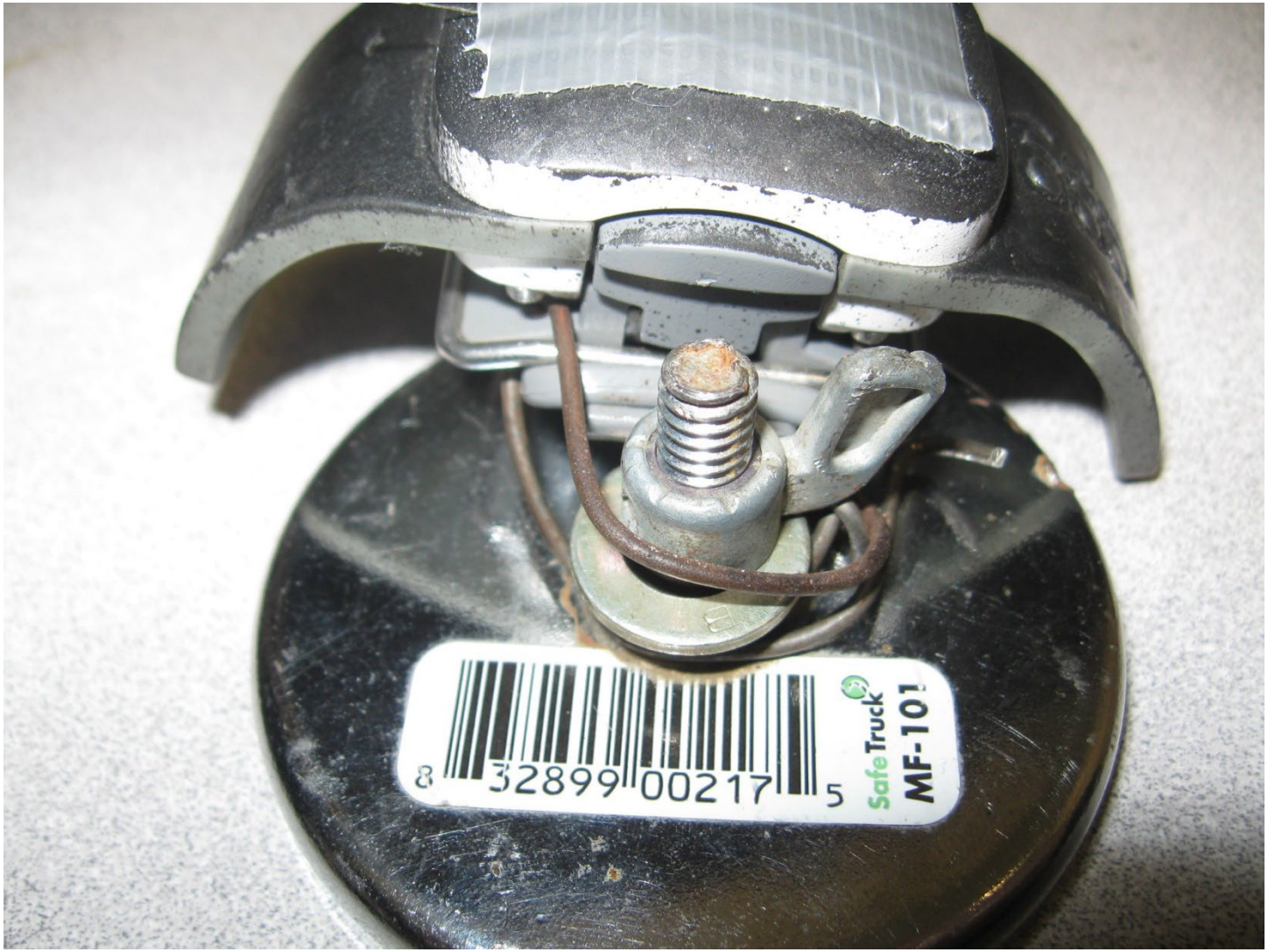
Location Tracking

LETTAC

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Global Positioning System (GPS) Devices

JUST TECH



JUST TECH


Bloodhound
THEFT TRACKER

tagg

How It Works Product Community

FEATURED ON

GOOD MORNING AMERICA abc NEWS FOX NEWS CNBC THE WALL STREET JOURNAL. WSJ The New York Times

GPS Documentation and Evidence

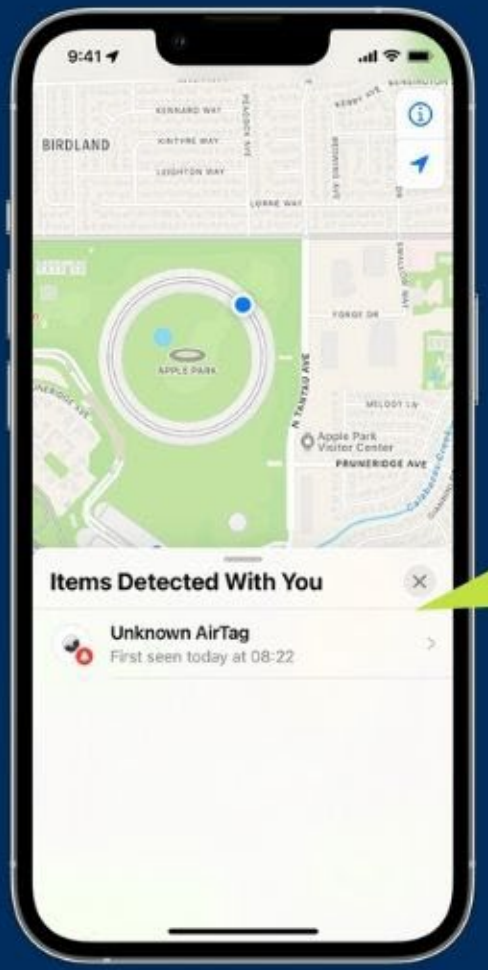
Computer	Phone	Financial Data
• Tracking software • Tracking websites	• Apps • Websites • Call-in numbers • Texts	• Equipment purchase • Real time tracking service charge

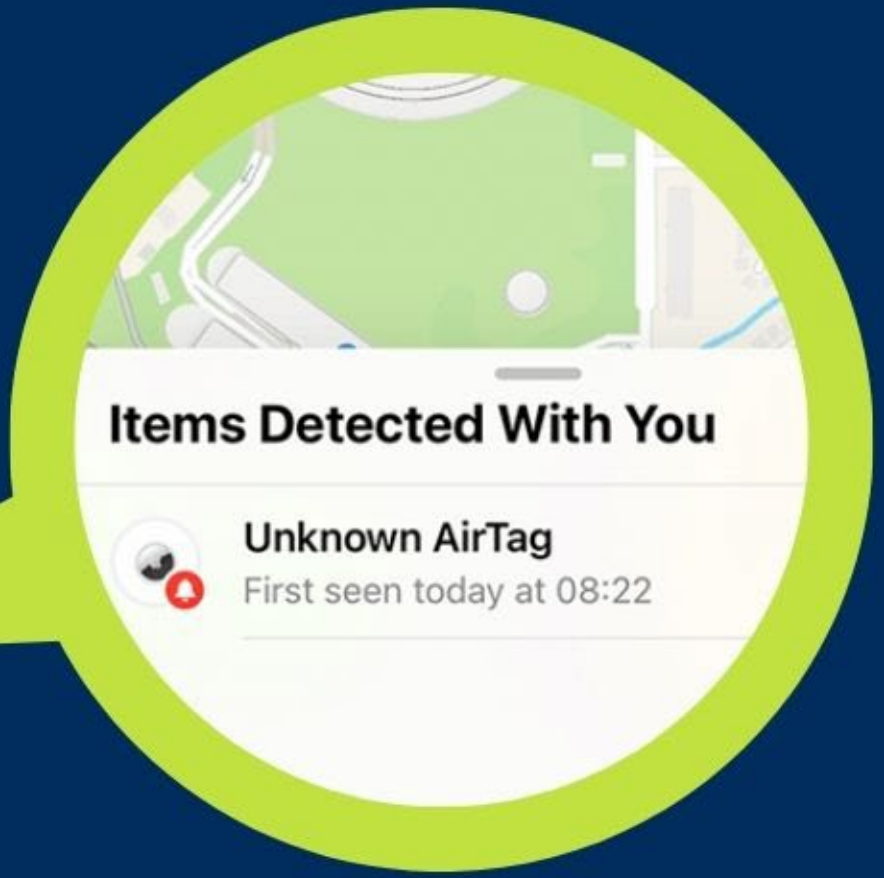
AirTags and Tile Devices

LETTAC

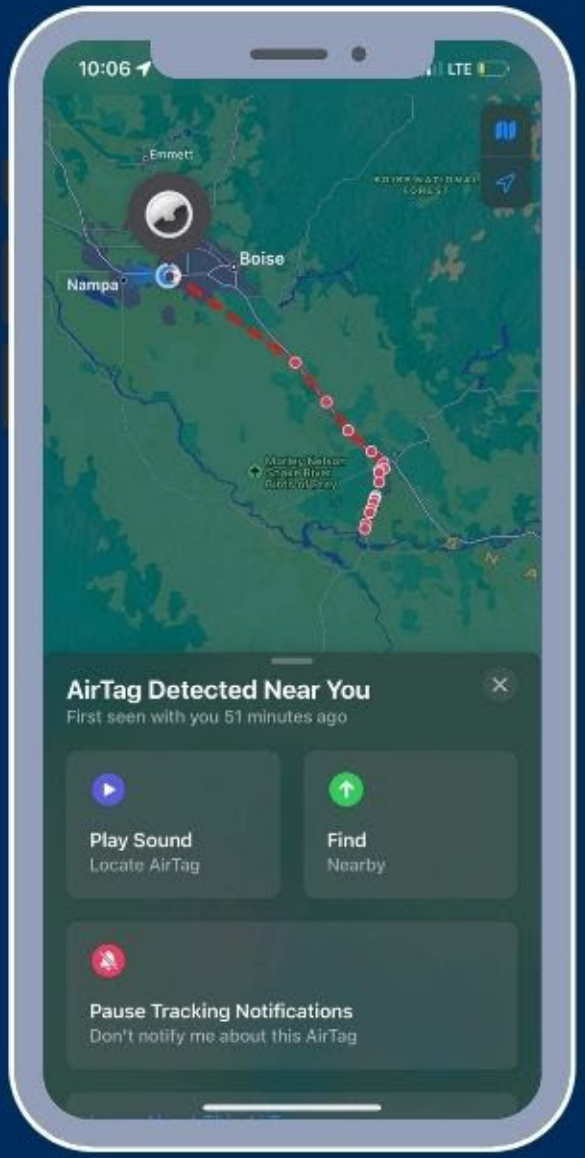
SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Apple Find My



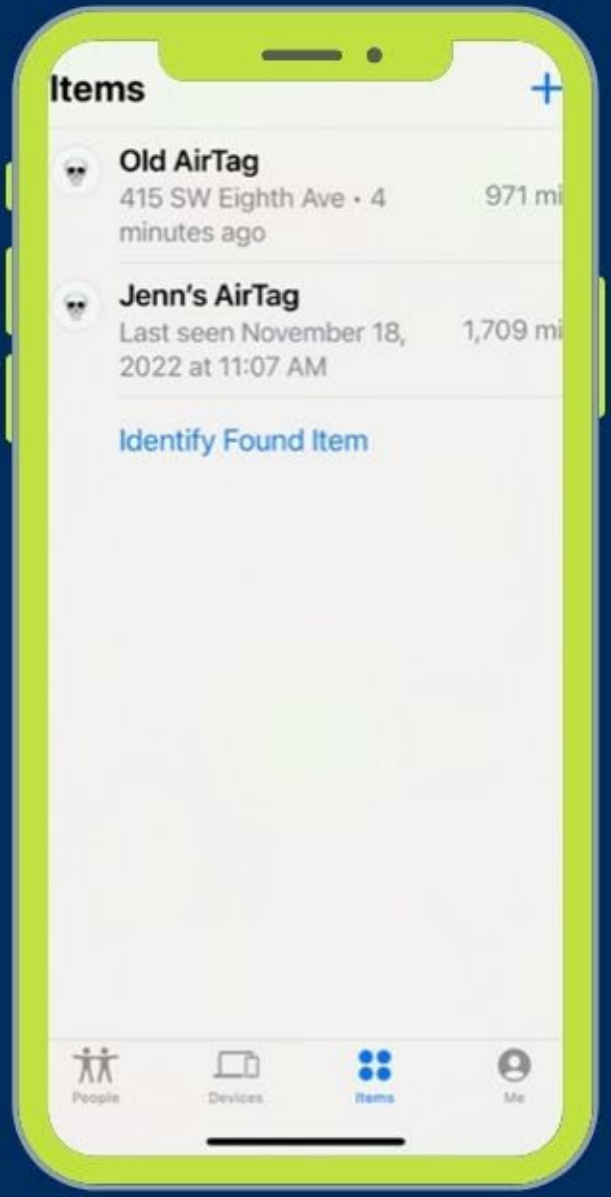


Victim's View

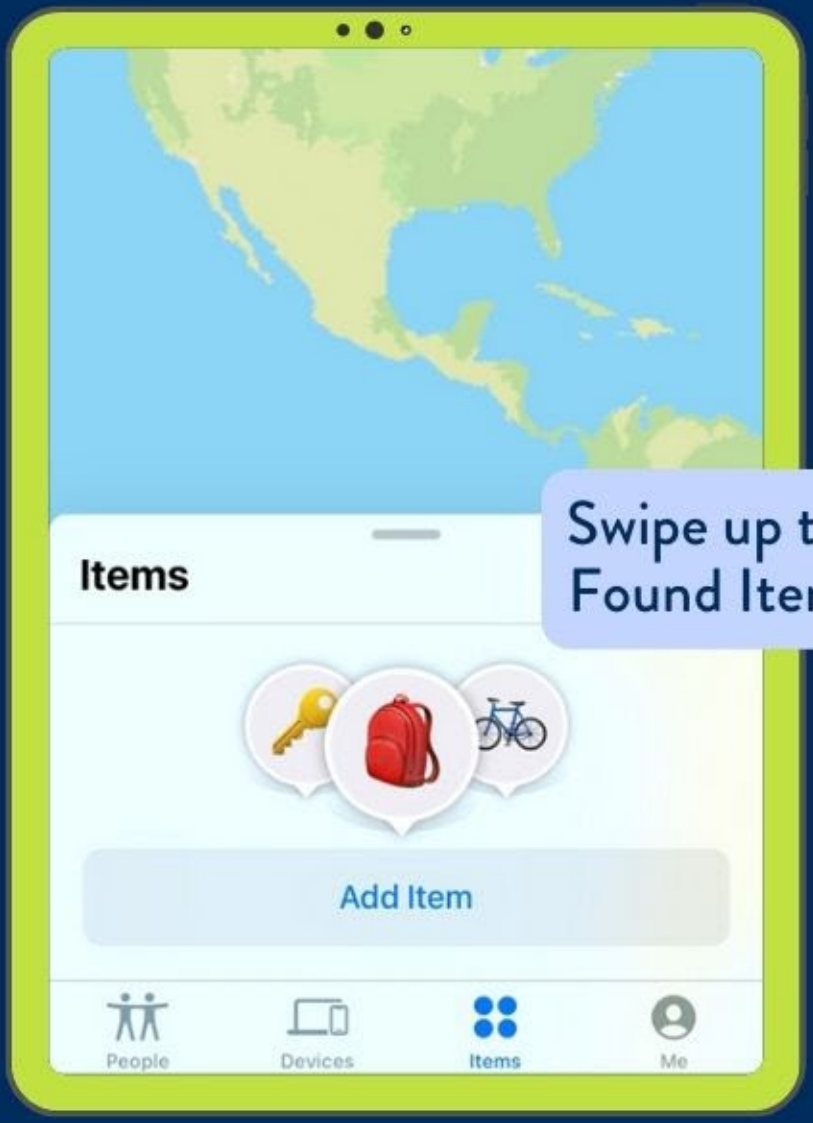



10:18
Search
LTE
FINDING
Steve's keys
11 ft

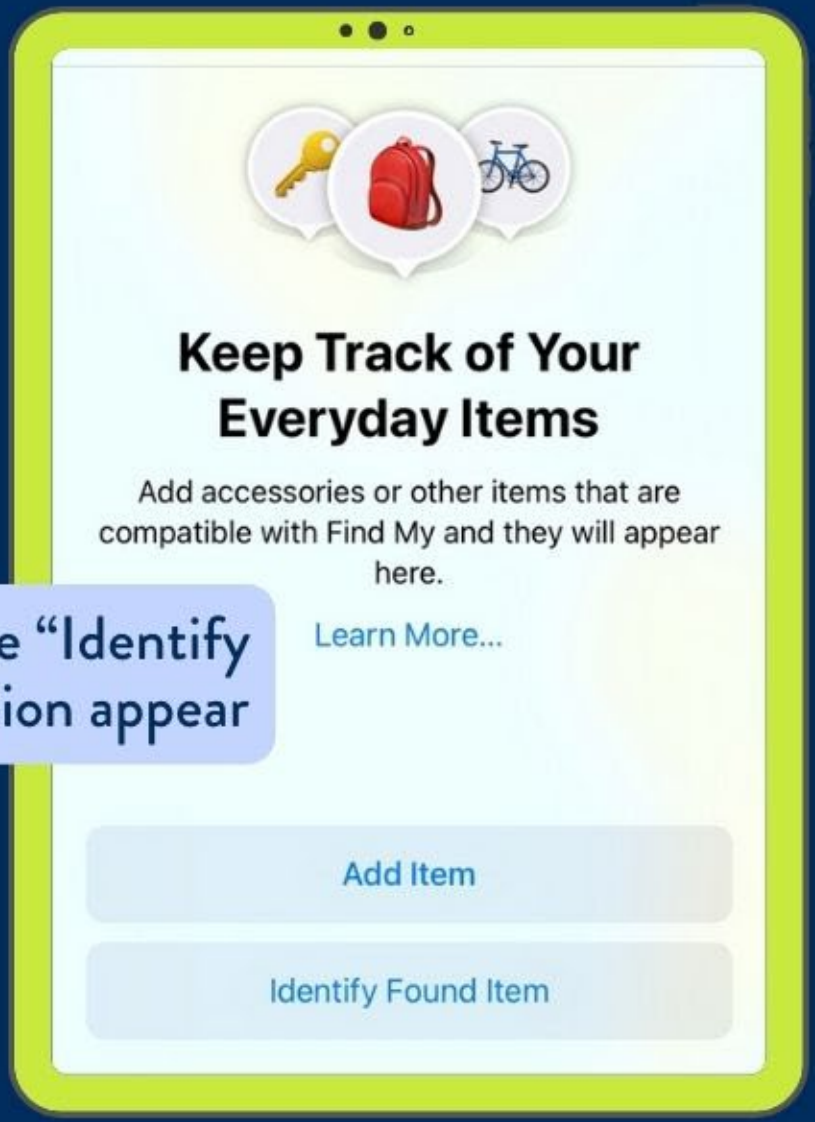
If you have items associated with your account



If you DO NOT have items associated with your account



Swipe up to make “Identify Found Item” option appear




Searching Items...
You can learn more about lost items, or see if the owner has left a message, by connecting to it.
If you found an AirTag, you can learn more by holding the top of your iPhone over it until a notification appears.


9:41
About This AirTag
Serial Number: ABCDE12FG345
Owner: (***) ***-6789
An AirTag is used to keep track of everyday items like keys or a bag.
The serial number is registered to the owner of this AirTag. If this AirTag is not familiar to you, learn how to disable it and stop sharing your location.
Instructions to disable ›
AA
found.apple.com

Non-consensual Distribution of Intimate Images

LETTAC

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Nonconsensual Image Resources

#CCRI
Cyber Civil Rights Initiative

Image Abuse Helpline:
1-844-878-2274

CyberCivilRights.org

StopNCII.org
Stop Non-Consensual Intimate Image Abuse

C.A.GOLDBERG
VICTIMS' RIGHTS LAW FIRM
www.cagoldberglaw.com

DMCA
DEFENDER
DMCADefender.com

Safety Strategies

LETTAC

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Safety Planning

- Social media presence: be practical and understand how to be the most secure with survivors (is it really private?)
- Finding trackers and tracking apps
- SmartHomes and account information
- New email account for evidence
- Documentation, reporting, and validation- safety planning is perhaps most important for mental health.

Basics of Tech Safety Planning

- Include technology as part of core safety planning
- Ask guided questions that are grounded in behaviors, tactics, and concrete elements of the relationship, to help survivors remember to think about their technology

Tech Issues After Family Separation

Many victims stay in their home and are navigating separation that includes child custody or one party moving away from the other.

Examples:

- Who set up devices? Who bought/gifted the victim watches, headphones? Who pays the utilities that charge devices?
- Are there children involved who have electronic devices?
- Will the victim be staying in one or more physical location(s) that the stalker had access to?
- If moving, will the victim be leaving behind phones, tablets, computers?

Help Map Out Devices

- A large part of tech services is helping victims remember devices!
  - When you ask about what technology they use, victims often just say “my phone”
- Give examples. Frequently forgotten:

Old Devices Still in Home

Shared Desktop Computers

Gifted Devices

Help Map Out Devices

Headphones

Watches

Children's Devices

Cameras

Smart Home Devices

Laptops & Tablets

Old Devices Still in Home

Shared Desktop Computers

High-Risk Scenarios

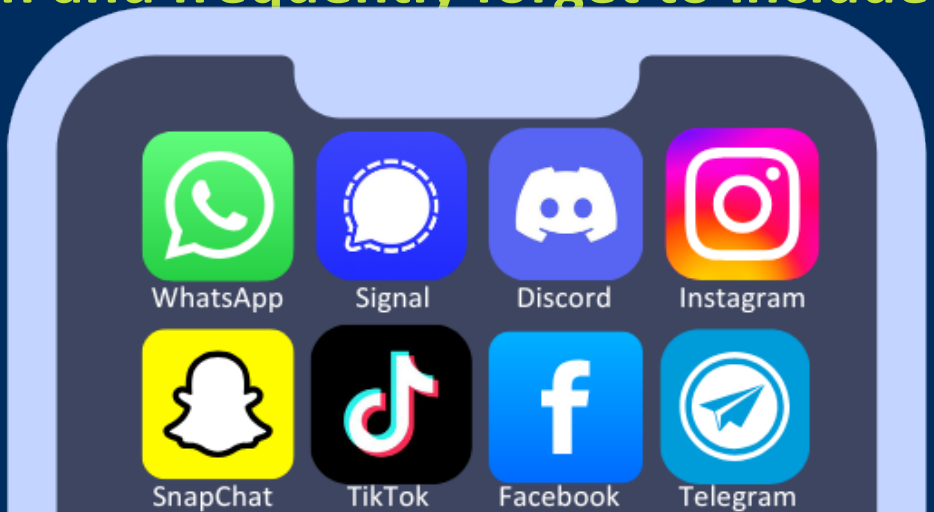
- Highest risk scenarios are often when a survivor is planning an exit, moving through a shelter service, or trying to obtain long-term protections.

- The two biggest tech concerns are typically **safe communication** and **location**.

Establishing Safe Communication

- What does the survivor use to communicate? An iPhone, an Android? Do they EVER share information via social media apps like WhatsApp or Instagram?
- Do you have access to resources to secure those methods OR can you help the survivor set up safe methods of communication?

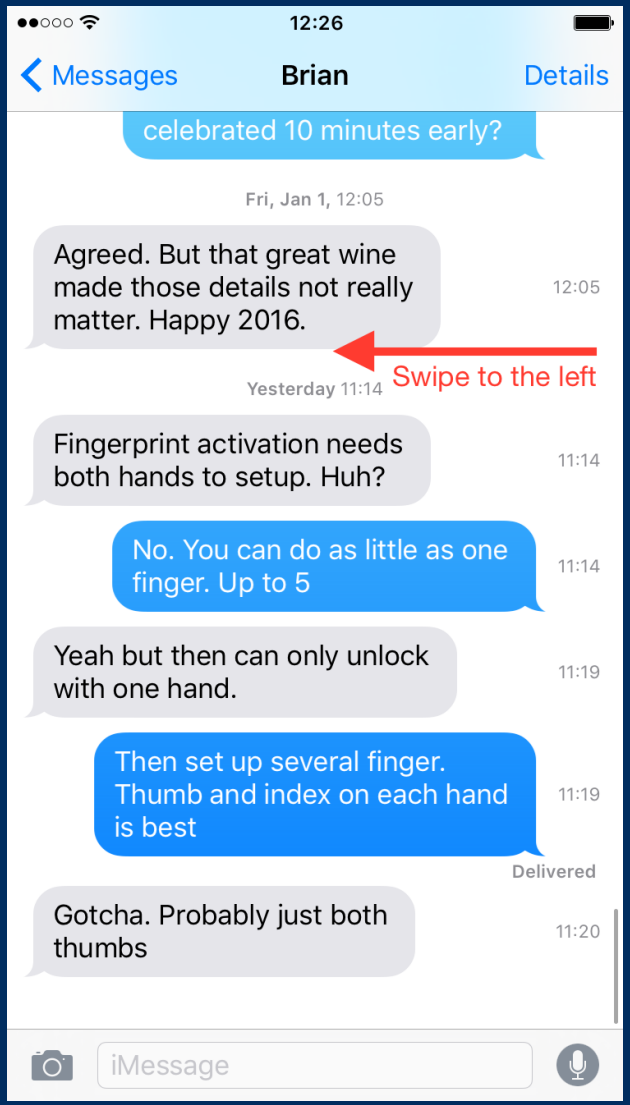
Survivors often need to be prompted about methods of communication and frequently forget to include key elements.



Establishing Safe(r) Communication

- Option 1: Secure the victim's existing communication methods
  - Will require moderate comfort with technology, at least enough to walk through a guide
- Option 2: Create a parallel communication method
  - Treat all other digital communications as unsecure
  - Typically do not want to get rid of existing methods (why?)

Tips for Documenting



1) Capture the whole screen, and don't crop, edit, or otherwise alter screenshots or images

2) Try to include a timestamp for messages

3) If a phone number is involved, delete the contact card to show the phone number, not a nickname

4) Look up the phone carrier and any other related information you can get for free

5) Keep a well-organized and annotated log of screenshots

Evidence Considerations

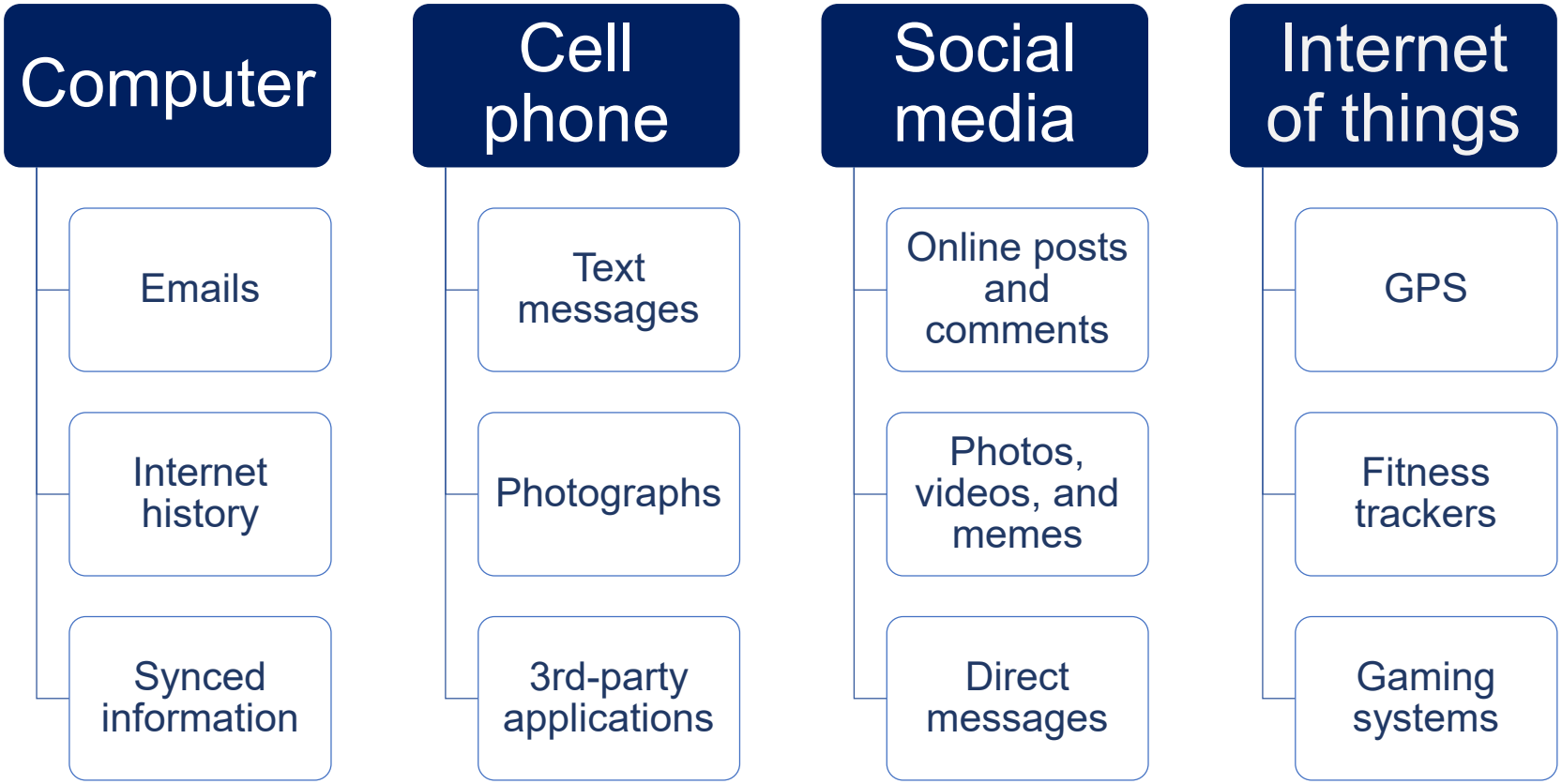
LETTAC

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Collecting Evidence

Whether a survivor is ready to file a report or not, collecting evidence keeps that option open by establishing:

- course of conduct crimes like stalking and harassment
- the intention to cause emotional, financial harm
- nature of relationship ('reasonable expectation of privacy')
- which platforms might have additional evidence


Computer
Emails
Internet history
Synced information
Cell phone
Text messages
Photographs
3rd-party applications
Social media
Online posts and comments
Photos, videos, and memes
Direct messages
Internet of things
GPS
Fitness trackers
Gaming systems

Preservation Letters

- **IMPORTANT: If you are going to seek records through a court order or a search warrant, you should send a preservation letter as soon as you are reasonably certain you are going to seek the order or warrant**
- The federal code requires the provider to honor your preservation letter, so long as your request is not unusually onerous
- Unless your state has "opted-out" by law, your state can take advantage of this tool, which may be used by any "governmental entity"
  - **18 USC 3077(6)** means: "the Government of the United States, any State or political subdivision thereof, any foreign country, and any state, provincial, municipal, or other political subdivision of a foreign country"

Preservation Letters

1) **In general.—** A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
2) **Period of retention.—** Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

Subpoenas

- Subscriber information
- Transaction history
- IP addresses

Court orders

- Wiretaps
- GPS tracking
- Non-disclosure orders

Search warrants

- Cell phones
- Computers
- Social media
- Cell-site Location Information (CSLI)

NRCC

NATIONAL RESOURCE CENTER ON CYBERCRIMES AGAINST INDIVIDUALS

A PROJECT OF

AEQUITAS

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE

#CCRI Cyber Civil Rights Initiative

NW3C

Key Takeaways

- Include questions about dynamics around technology early on
- Help victims stay organized and document, document, document
  - Help consider all devices
- Basic checks are highly effective
  - Secure passwords, owning utility plans, and platform guided walkthroughs probably fix about 80% of fixable compromises
- "Narrow corridor": Be aware but grounded

Resources

- **Walkthroughs and Guides:**
  - Clinic to End Tech Abuse Guides (user-friendly)
  - Apple SafetyCheck
  - Google Security Checkup
  - Meta Privacy Center
  - Phone plans: Verizon, AT&T, T-Mobile
  - Right to Be's guide to online harassment
- **Non-consensual Intimate Images:**
  - Cyber Civil Rights Initiative
  - StopNCII.org

www.StalkingAwareness.org

- Practitioner guides
- Training modules
- Victim resources
- Webinars

Sign up for our Newsletter!

@FollowUsLegally

Sgt. Denise Jones

Clark County
Sheriff's Office

Law Enforcement Consultant

DJones@ClarkCountyOhio.gov

StalkingAwareness.org

SPARC
STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Jennifer Landhuis M.S.

Director

202-819-1391

Director@StalkingAwareness.org

StalkingAwareness.org

Training Evaluation

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

@FollowUsLegally