SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

The Use of Technology to Stalk

OVW Funding

This project was supported by Grant No. 15JOVW-22-GK-03986-MUMU awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

SPARC Website

- URL: www.StalkingAwareness.org
- Available resources include:
  - Practitioner guides
  - Training modules
  - Victim resources
  - Webinar recordings
- Sign up for our newsletter
- Follow us on Facebook, Instagram, and Twitter
  - @FollowUsLegally

The Use of Technology to Stalk

SPARC
STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Technology does not cause stalking.

Stalkers cause stalking.

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Technology & In-Person Stalking

- The majority of stalking victims experienced both in-person stalking and technology-facilitated stalking.

Reference: Messing, J., Bagwell-Gray, M., Brown, M.L., Kappas, A., & Durfee, A. (2020). Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. Journal of Family Violence 35(1): 693-704.

SLII Framework

Surveillance

- Smart home devices
- Tracking software
- Tracking devices
- Monitoring online activity
- Accessing online accounts
- Cameras or audio/video recording devices

Interference

- Spreading rumors online
- Doxing
- Posing as victim and creating harm
- Swatting
- Posting private photos, videos, information online, real or fake
- Using technology to encourage others to harm the victim

Life Invasion

- Unwanted contact online or through text messages, phone calls, or other platforms
- Impersonating victim
- Impersonating others to access the victim
- Hacking and/or controlling victim's accounts

Intimidation

- Online threats
- Blackmail
- Sextortion
- Threats to release private info, photos, or videos (real or fake)
- Threats to interfere with property, employment, finances, accounts

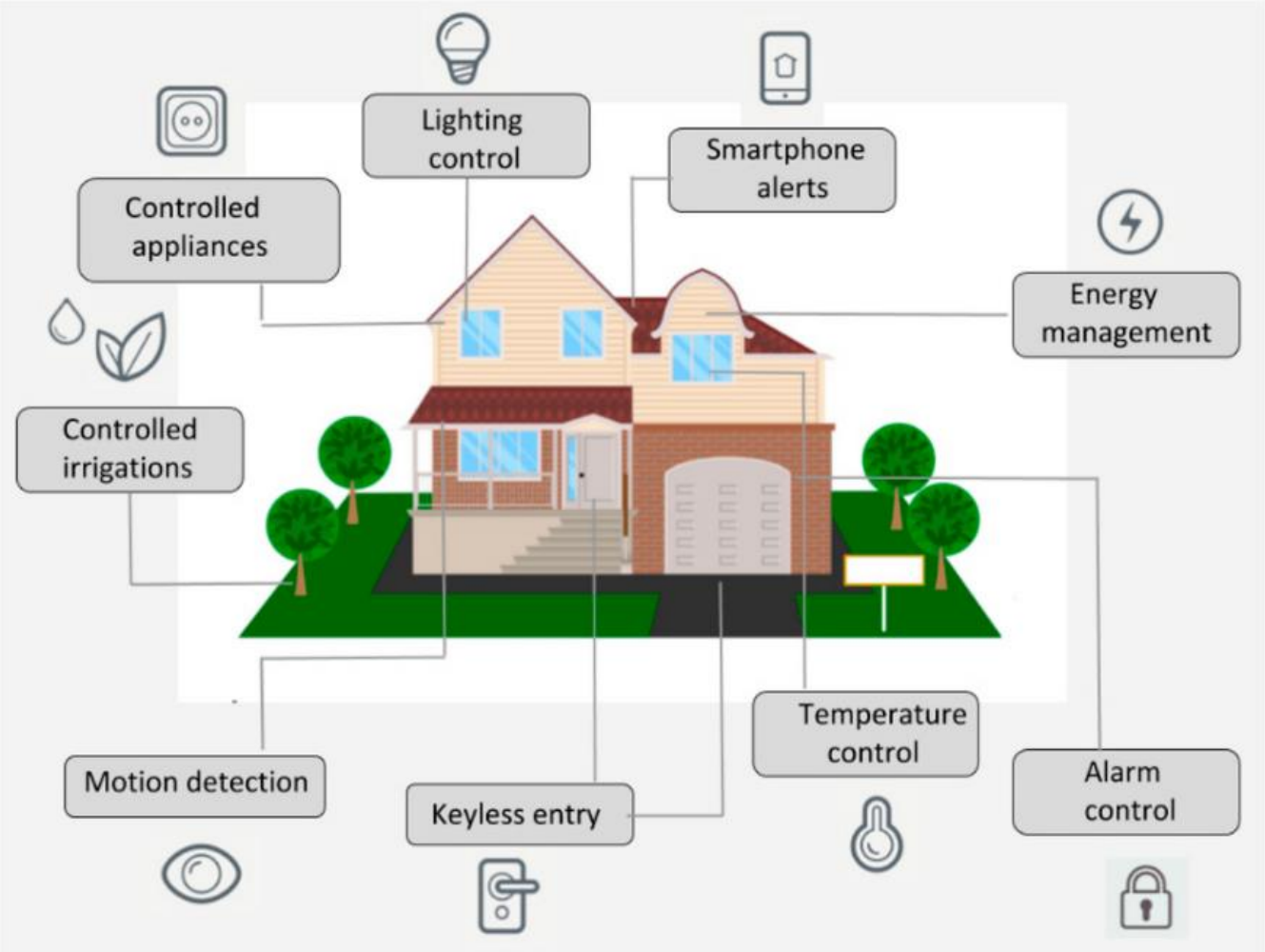
Common Technology Tactics Experienced by Stalking Victims

Tactic	% of Victims
Unwanted phone calls, voicemails, text messages	66%
Unwanted e-mails or social media messages	55%
Monitored activities using social media	32%
Posted/threatened to post inappropriate/personal info	29%
Spied on/monitored activities using tech	22%
Tracked location with electronic device or app	14%

Reference:

Truman, J.L., & Morgan, R.E. (2022). Stalking Victimization, 2019. Washington, DC: US DOJ, Bureau of Justice Statistics, Special Report.

Smart Home capabilities



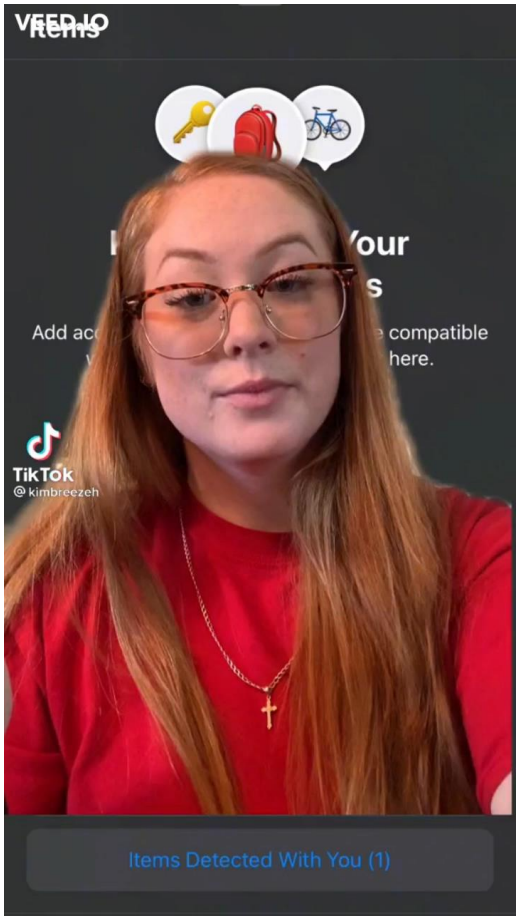
Tracking Location

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

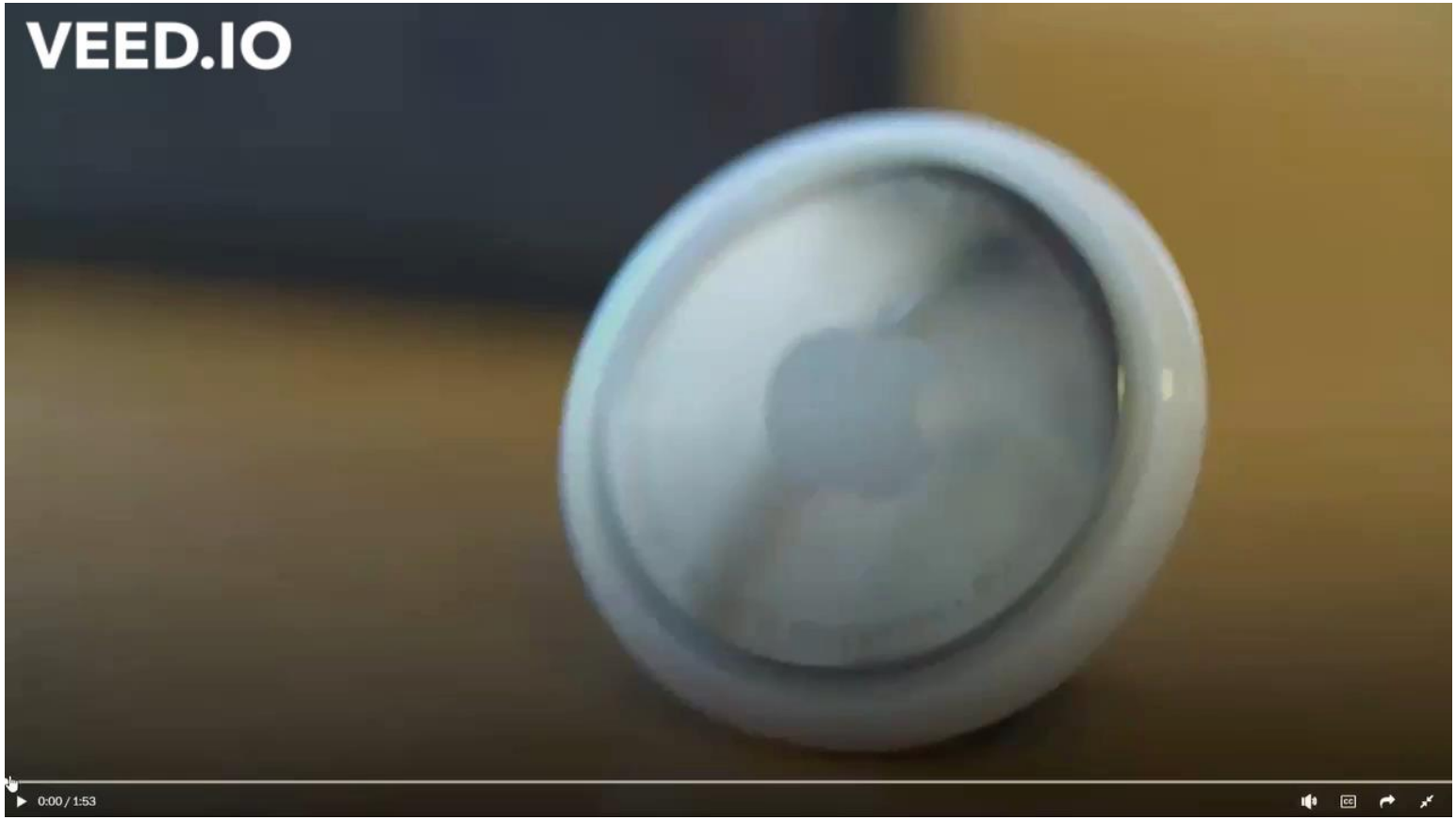
How Do Stalkers Track Location?

- Property Tags
- Family Trackers
- Access to and/or Shared Victim Accounts
- Social Media Maps/Check-ins
- Installed Stalkerware
- Proxy Stalking

AirTag Case Study



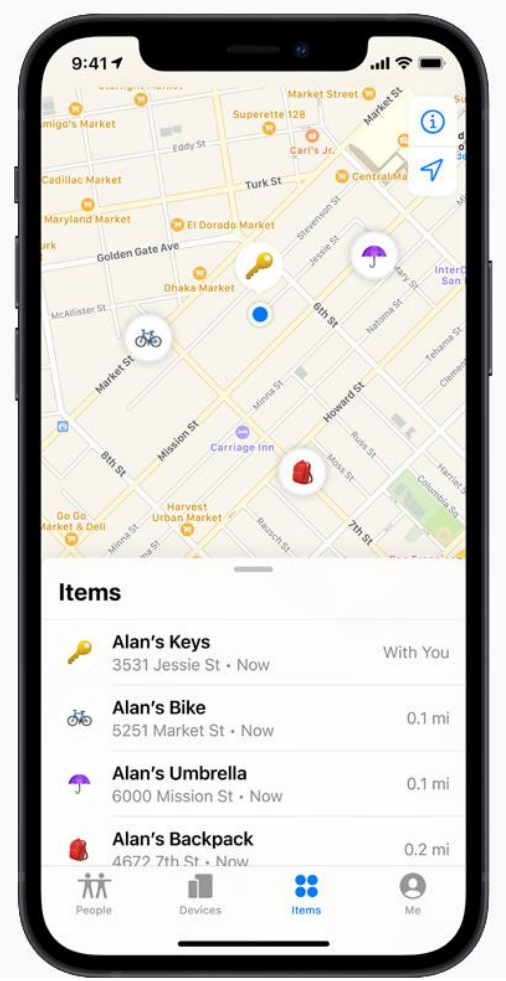
AirTag Explainer Video



Note: Notification time is now a few hours, NOT 3 days
Android now has an automatic AirTag tracker

Understanding AirTags

- Shows current location, not location history
- Frequency of the location update varies
  - Depends on other devices in range
- While Tile requires people to have downloaded the Tile app for the location tracking to “ping,” AirTag “pings” off any Apple device within 800 feet

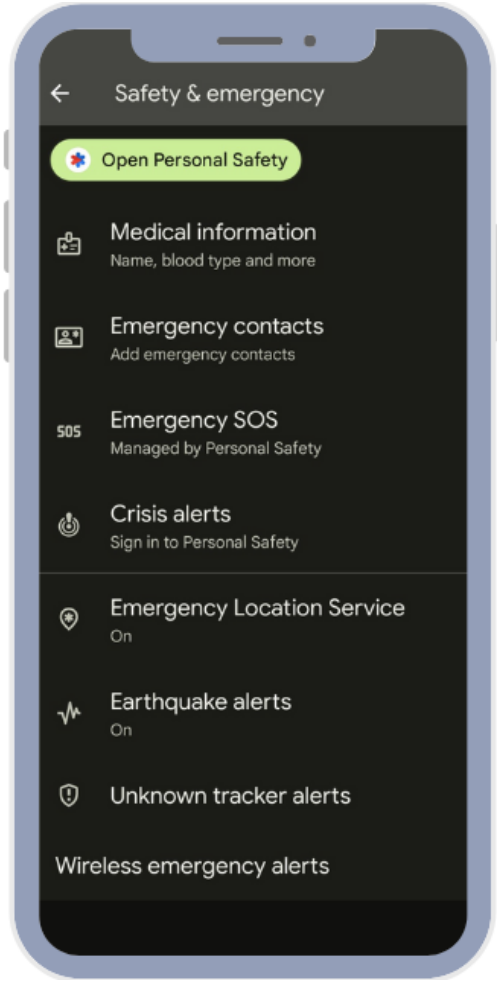


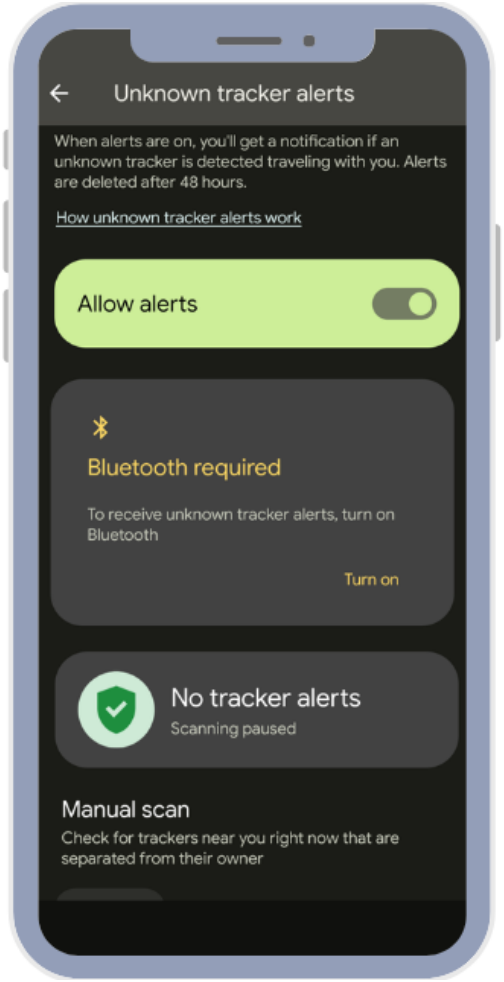
Notification Limitations

- Alerts are inconsistent and designed to catch when device is traveling with the victim
- Most users are notified when they return home, not while traveling
- If the offender is present and/or in close proximity to victim regularly, notification is unlikely

AirTag Alert Settings: Android

android

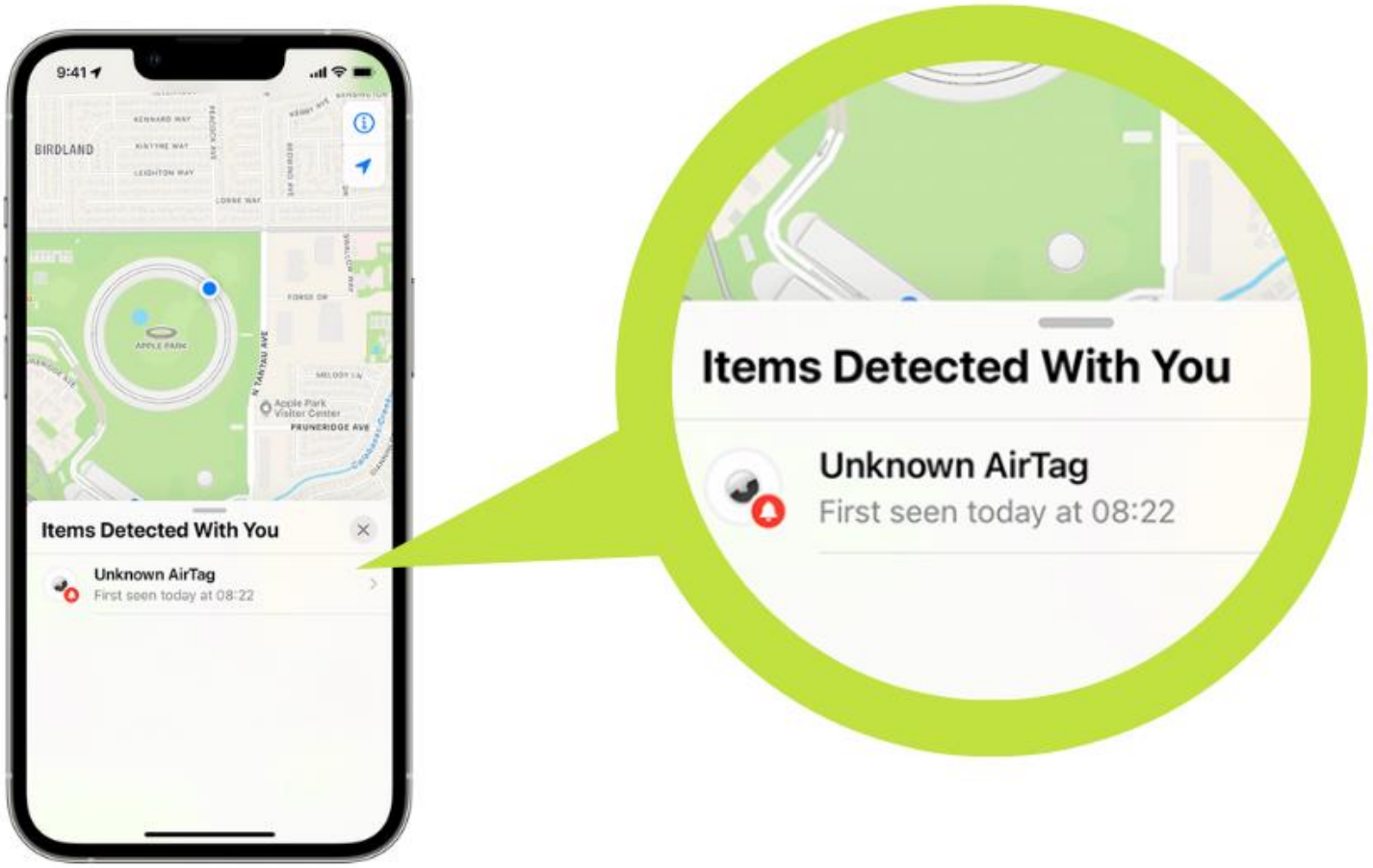




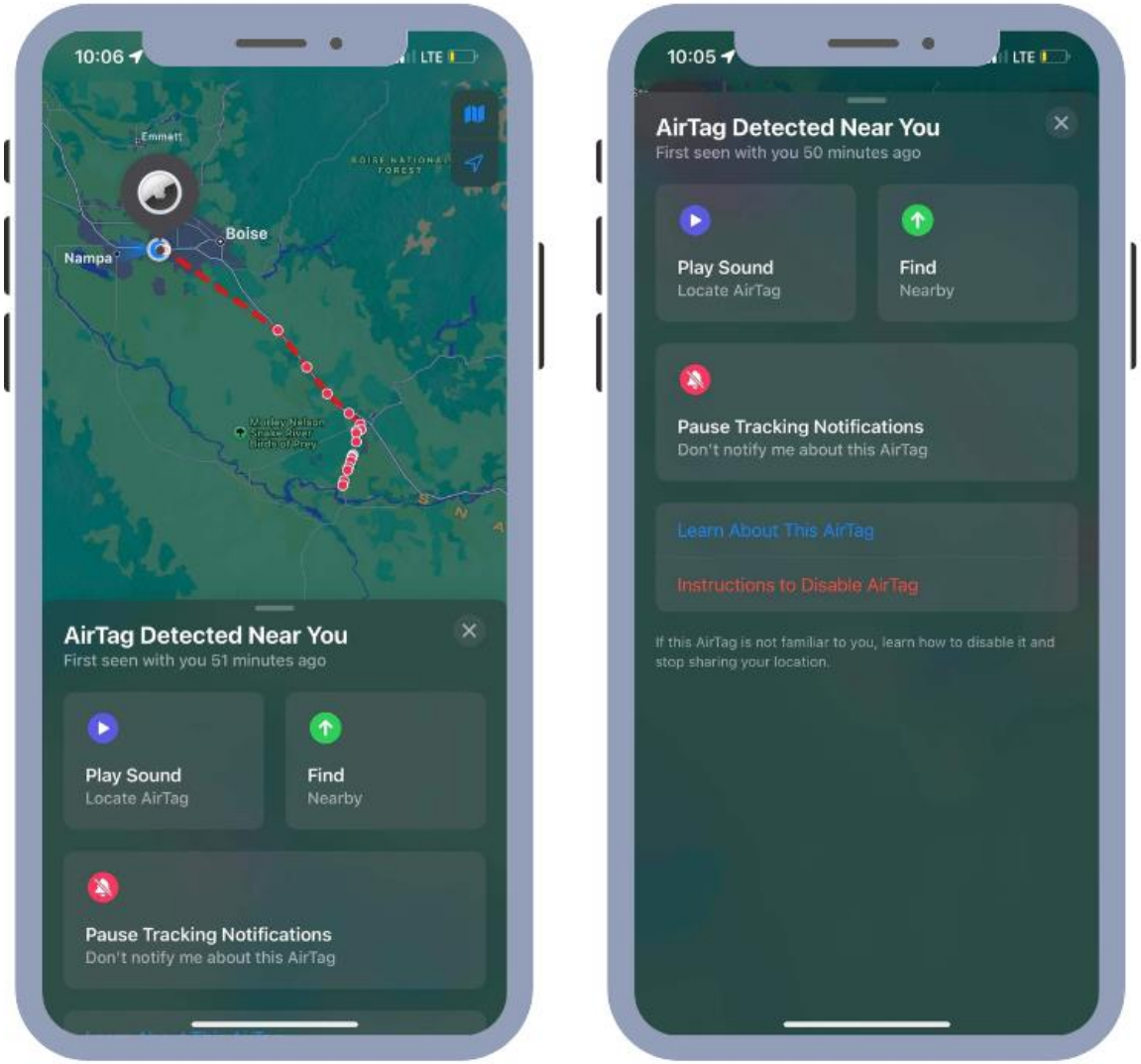
AirTag Alert: Android

- App called Tracker Detect
- Can be downloaded from the Play Store

AirTag Alert: Apple

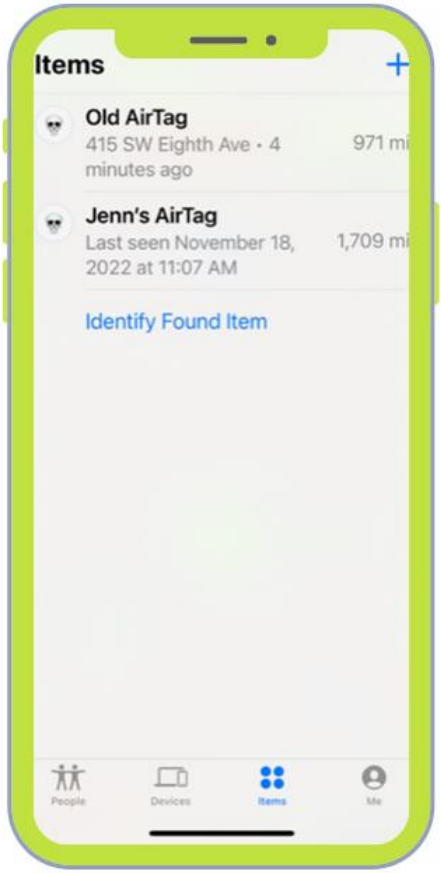


Victim View in “Find My”



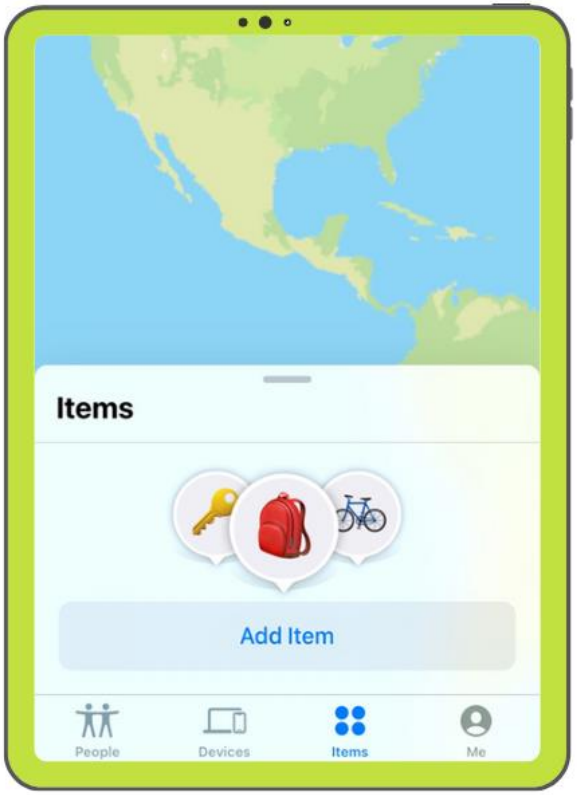
Apple Users: Open “Find My” App

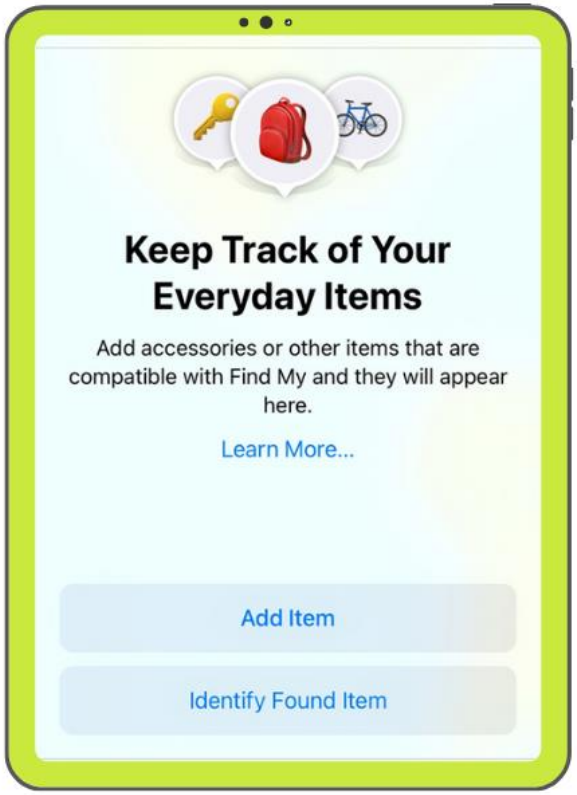
“Find My” Account With Items



- If you have items associated with your account, this is what you see
- This is what the offender would see for any AirTag they set up

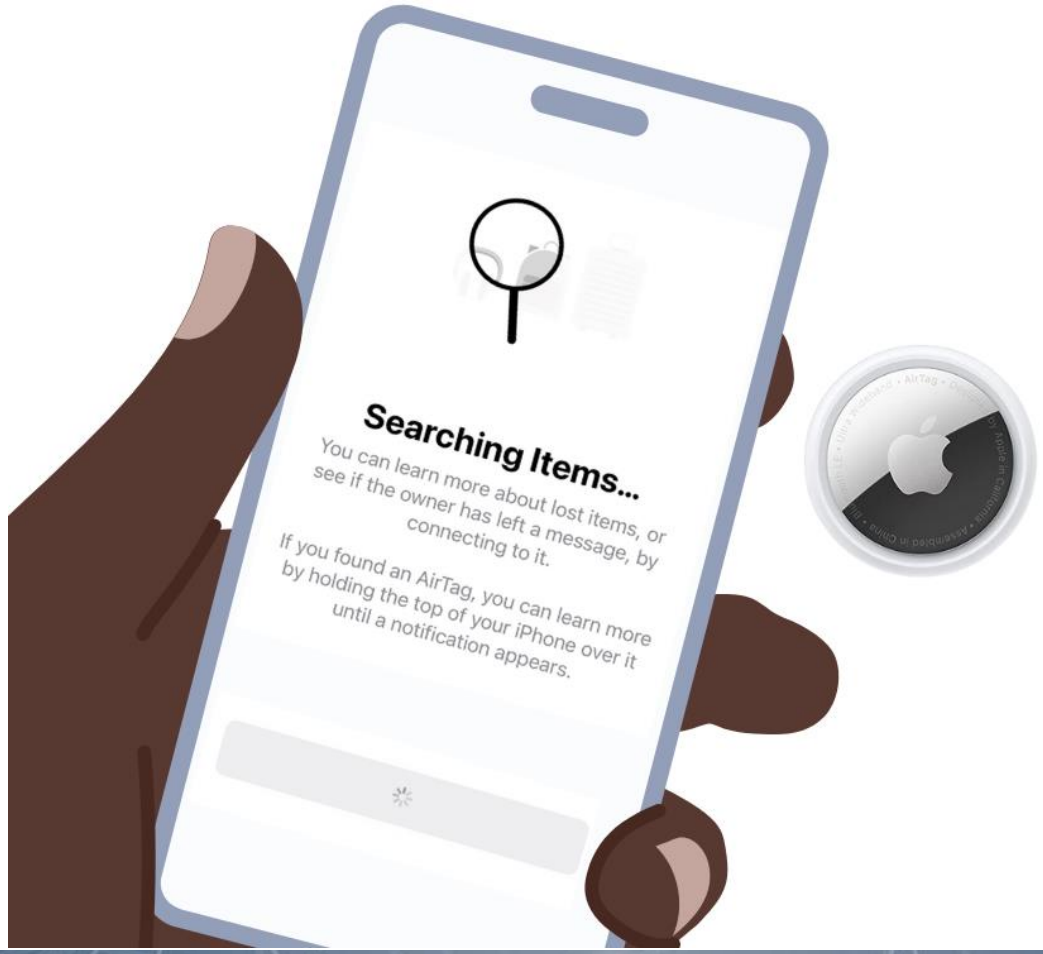
“Find My” Account Without Items



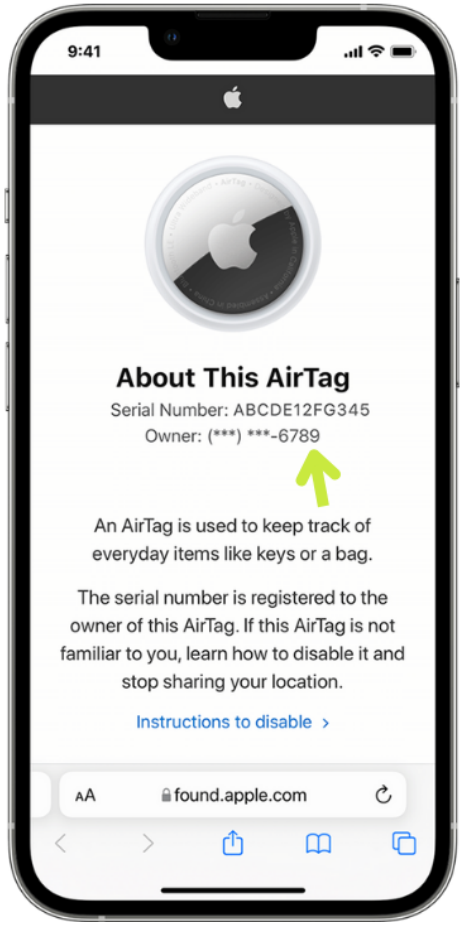


- Swipe up to make “Identify Found Item” option appear

Hold iPhone Over a Found AirTag



“Find My” Provides Info about Found AirTag



Disabling AirTag

- Opening the AirTag to view the serial number disables the Tag – thereby alerting the offender that it's been found
  - Law enforcement should come to victim and consider faraday bag
- Turning off Bluetooth will NOT stop the device from emitting a signal to the offender
- Take screenshot for evidence

Evidence with AirTags

- Serial number is unique to each AirTag
- Serial number is on physical device, but will not show up on phone
- Contact email: lawenforcement@apple.com to check device registration
- Check financial records of suspect
- Contextual evidence

Global Positioning System (GPS) Devices

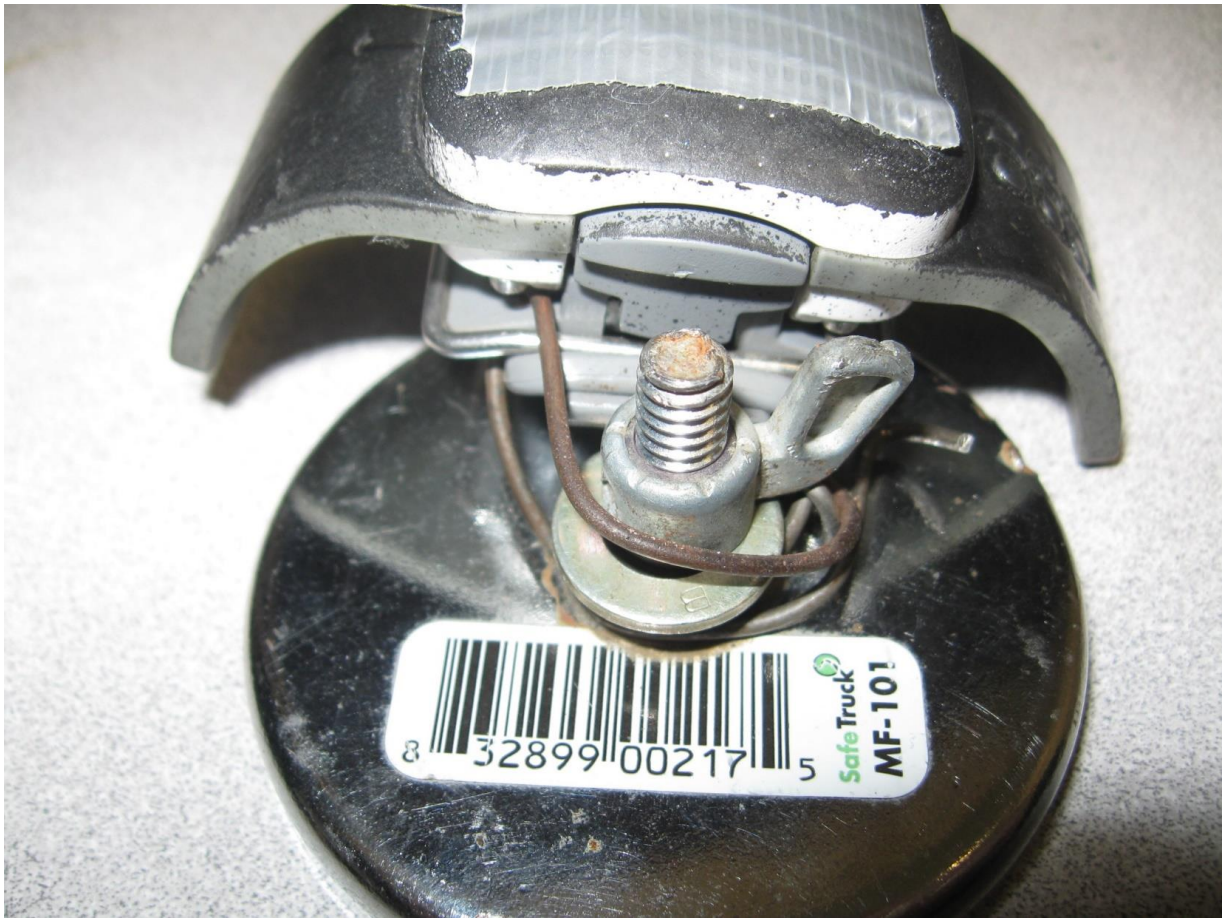
- Global navigation satellite system that tracks location and other things

Child Trackers & Pet Trackers

- GPS devices are often marketed for keeping track of your kids or pets

Pet Tracking Device (1 of 2)

Pet Tracking Device (2 of 2)



Location Sharing

- May be coerced
- Victim may not realize they are sharing their location
- A stalker may utilize multiple methods/applications to track their victims

Percentage of People Checking In or Sharking Their Location by Platform and Privacy Settings

Platform	Private	Public
Facebook	57.1%	42.9%
Instagram	43.5%	56.5%
Snapchat	60.9%	39.1%
Twitter	26.5%	73.5%

- Nearly 1 in 4 people felt it's extremely or moderately safe to share their location on social media.
- 30.7% of people with Snapchat shared their location on the Snapchat map.

Reference:
2020 ADT LLC dba ADT Security Services. https://www.adt.com/resources/location-services-risks

Spoofing

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

SpoofCard Video

Spoofing: What You May Hear

- "Numbers I don't recognize call and harass me."
- "I keep getting hang-up calls from random numbers."
- "It shows up as my mom/friend/someone I know, but it is the offender calling."
- "I know it's the offender, but it doesn't sound like them."
- "I blocked the offender, but they just keep calling me from different numbers."
- "People are saying I called them, but I didn't."

SpoofTel


SPOOFTEL
THE WORLD'S LEADER IN CALLER ID SPOOFING
username
password
go
forgot password
Free Call
Rates
FAQ
Apps
Developers
Contact
Sign Up
FREE CALLER ID SPOOFING TRIAL
It is more important than ever to protect your personal information and it all starts with a telephone number. A caller ID spoofer allows you to tweak how your phone number shows up through incoming calls.
It has never been easier to fake caller ID displays, maintaining your privacy and protecting your information. When you want to spoof a call, it involves more than a changed number. At SpoofTel, our services come along with a voice changer option.
Your Number
1
Enter the number you are calling from
Destination Number
1
Enter the number you would like to call
Spoof Number
Voice Pitch
Adjust the pitch of your voice
Soundboard
None
DLPERX
Copyright © 2004 - 2020 SpoofTel Ltd. - All Rights Reserved.
Like
Save
Tweet

Spoofing

- Offenders spoof number victim will answer
- Offenders spoof victim with court, police or other numbers victim will answer
- Offenders believe we can’t prove they spoofed the call

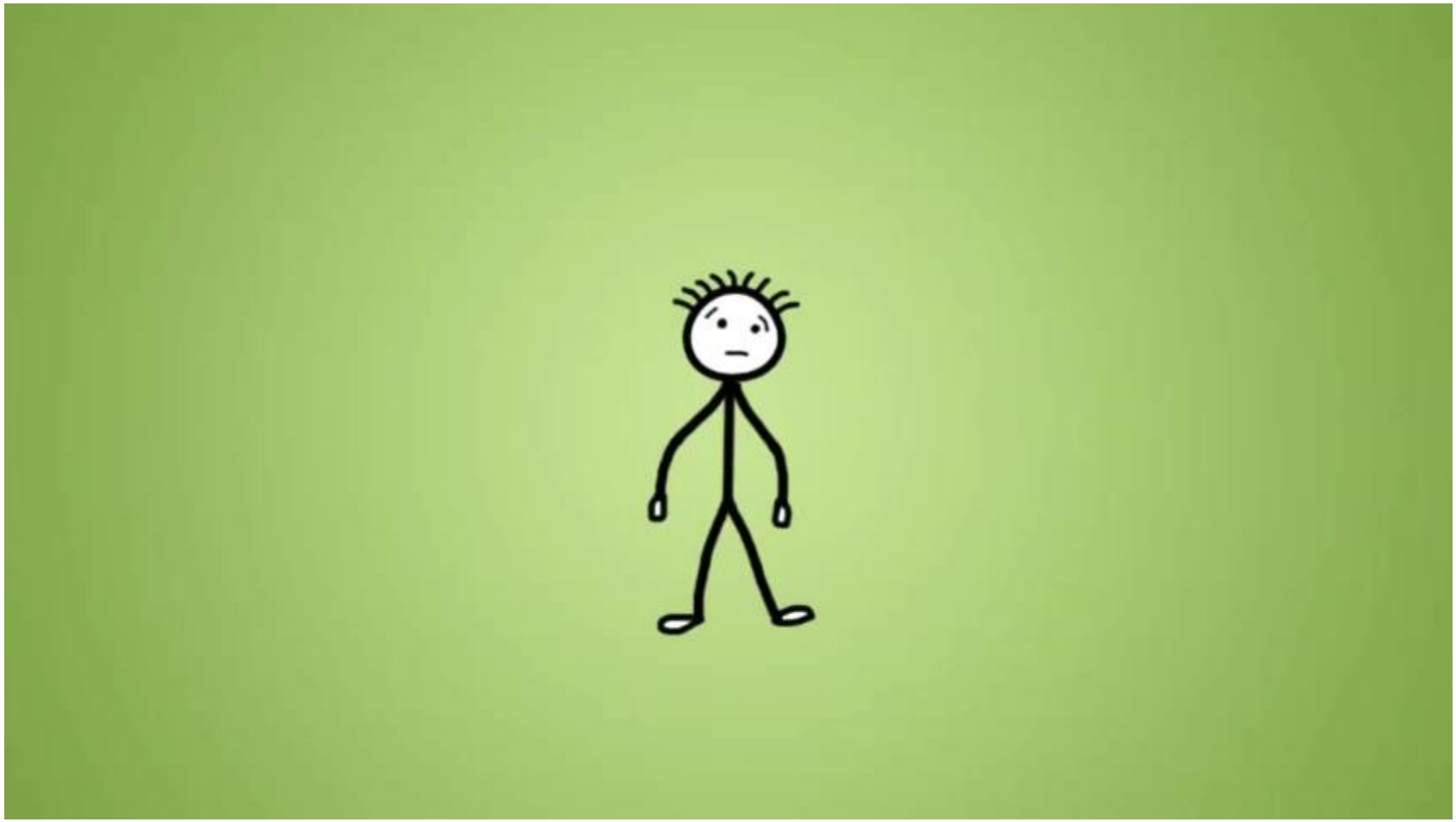
Documentation with a SpoofCard

- Phone records from: victim, “friend”, and suspect
  - Victim’s records show “friend” called but friend’s records show no call
  - Suspect’s records show a call to SpoofCard
    - Call the number and record
- Financial records of suspect

Stalkerware

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Cell Phone Spyware Video



Stalkerware: What You May Hear

- "They hacked my phone."
- "They hacked my account(s): e-mail, Facebook, Instagram, Snapchat…:
- "They're reading my texts."
- "They are listening to my calls."
- "They seem to know everything I've done on my phone."
- "They know my passwords and logins, even though I just changed them.
- "They have and/or are referencing pictures of me I took on my phone."
- "They keep showing up where I am."

What is Stalkerware?

- Commercially available software used for spying
- Made for individual use
- Typically hides itself from the list of installed programs and does not display any activity notifications

About Stalkerware

- Physical access to the device is almost always required for installation
- Can be on both Apple and Android devices, but more common on Android
- Best to assume all activities on device are being monitored

Removing Stalkerware

- All actions may cause potential safety concerns!

- Factory reset
  - Note: this also destroys the evidence
- Change passwords on all apps/accounts when re-installed
- Antivirus can sometimes remove stalkerware

Non-Stalkerware Possibilities

- Sharing Settings
  - Phone login and password security
  - Cloud/Account Backup
  - Family sharing, "Find My Device"
- Account Access
  - Individual accounts: e-mail, social media, dating websites
  - Smart device accounts
  - Previously shared accounts
- Other Tools
  - Devices: GPS tracker, key logger, cameras, recording devices
  - Friends, family, colleagues

Public Data

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Geotagging

- Camera + GPS = Geotagging

Exif Viewers Show Geo-Info

- Exif = Exchangeable image file format
- Descriptive data (meta-data) in an image file that include the date the photo was taken, resolution, shutter speed, focal length and geolocation

EXIF Data

http://regex.info/exif.cgi

Jeffrey's Exif Viewer

From Web / From File — Image URL: [ ] View Image At

Basic Image Information

Target file: IMG_7655[1].JPG

Camera:	Apple iPhone 6
Lens:	iPhone 6 back camera 4.15mm f/2.2 Shot at 4.2 mm Digital Zoom: 2.362934363×
Exposure:	Auto exposure, Program AE, 1/30 sec, f/2.2, ISO 200
Flash:	Off, Did not fire
Date:	**March 2, 2016** 7:50:32PM (timezone not specified) (1 hour, 31 minutes, 8 seconds ago, assuming image timezone of US Pacific)
Location:	Latitude/longitude: **38**° 58' 1.9" North, **92**° 22' 26.2" West (38.967208, -92.373947) Location guessed from coordinates: *2200 Interstate 70 Dr SW, Columbia, MO 65203, USA* Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 223 meters (731 feet) Camera Pointing: South
File:	**3,264** × **2,448** JPEG (**8.0** megapixels) 1,193,426 bytes (1.1 megabytes)
Color Encoding:	**WARNING:** Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly.** Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Viewing EXIF data

- Online exif data viewers
- Apps
- Right click on the photo on a desktop and go to properties-details

Safety Strategies

- Turn location “off” on cell phone camera
- Review social media site to determine if exif data can be viewed
- Remove exif data using an online exif data removal tool

Google Web & App Activity Settings

Web & App Activity

Your Web & App Activity includes the things you do on Google services, like Maps, Search, and Play. It can also include things you do on sites, apps, and devices that use Google services or your voice and audio recordings. The activity you keep is used to give you more personalized experiences, like faster searches and more helpful app and content recommendations.

You can see your activity, delete it manually, or choose to delete it automatically using the controls on this page. Learn more

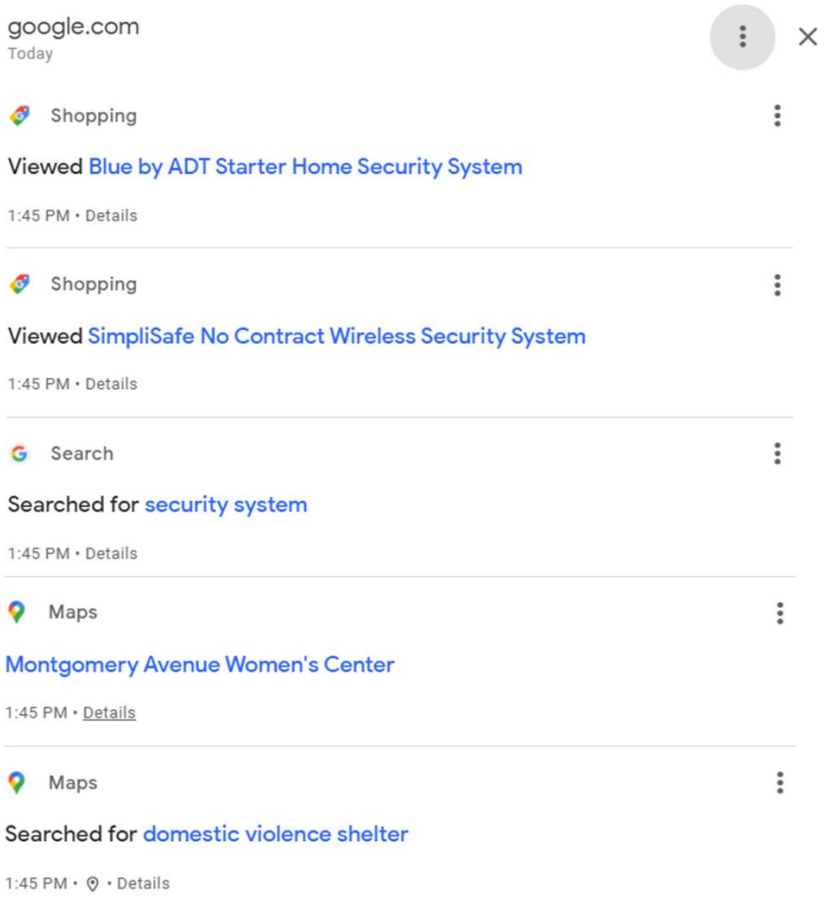
Saving activity
Your Web & App Activity is on
Saving audio is off

Auto-delete (Off)
Choose an auto-delete option

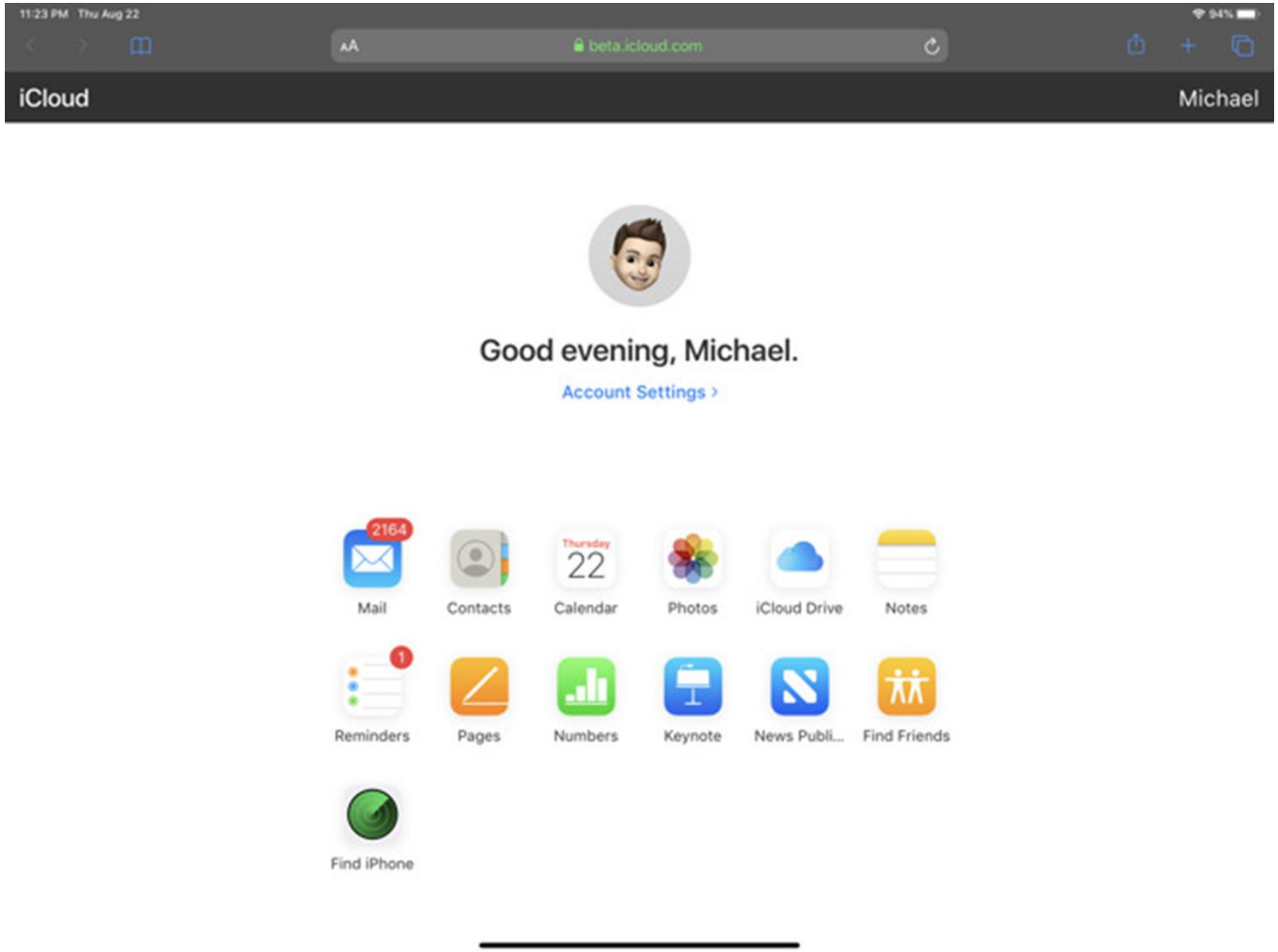
Google protects your privacy and security. Manage My Activity verification

Search your activity

Web Activity History



iCloud Access from a Browser



Find Yourself…

- URL: www.FastPeopleSearch.com
- URL: www.TruePeopleSearch.com
- URL: www.PeopleSearchNow.com

Non-Consensual Distribution of Intimate Images

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Sexually Explicit Photos

16% of victims 18-24 years old report that the stalker shared nude, semi-nude, and/or sexually explicit phots of videos of them.

Reference:
Brady, P.Q. & Woodward Griffin, V. (2019). The Intersection Stalking and Sexual Assault Among Emerging Adults: Unpublished Preliminary Results. mTurk Findings, 2018.

Deepfake Apps

- New AI deepfake app creates nude images of women in seconds
- The resulting fakes could be used to shame, harass, and intimidate their targets

Resources for Non-Consensual Distribution of Intimate Images

- Cyber Civil Rights Initiative (#CCRI)
  - URL: www.CyberCivilRights.org
  - Image Abuse Helpline phone number: 1-844-878-2274
- Stop Non-Consensual Intimate Image Abuse
  - URL: www.StopNCII.org
- C. A. Goldberg Victim Right's Law Firm
  - URL: www.cagoldberglaw.com
- DMCA Defender
  - URL: www.DMCADefender.com

Technology-Facilitated Stalking and Sexual Assault

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Sexual Assault, Stalking, and Technology

- Offenders use technology to facilitate and cover up sexual violence
  - Using platforms to find and groom victims (messages, online communities)
  - Gifts that monitor or allow access
- Misusing access to publicly available data to gain information
- Threats to disseminate intimate images
  - Including those acquired through surveillance cameras
- Sexual exploitation/trafficking via tech

Technology-Facilitated Sexual Assault Headlines

- Jebidiah Stipe, Wyoming Marine, Solicited Ex-Girlfriend's Rape And Assault On Craigslist
- Details emerge in Web rape case: California Marine also tried to solicitate rape of ex-wife, authorities say
- Judge gives man 60 years in Craigslist rape case

Dating App Facilitated Sexual Assault (DAppSAs)

- 14% of the 1,968 rapes committed by acquaintances occurred during an initial meetup arranged through a dating app
- High percentage of victims with self-reported mental illness (59.6%)
- More violent sexual assaults than acquaintance sexual assaults
  - Increased strangulation (32.4%); assaultive/penetrative acts; and victim injuries, especially anogenital and breast injuries
- "Due to the increased violent nature of DAppSAs, the researchers propose that sexual predators use dating apps as hunting grounds for vulnerable victims."

Resource:

Valentine, J.L., Miles, L.W., Mella Hamblin, K., & Worthen Gibbons, A. (2023). Dating App Facilitated Sexual Assault: A Retrospective Review of Sexual Assault Medical Forensic Examiation Charts. Journal of Interpersonal Violence, 38(9-10), 6298-6322.

Dating App Concerns

- Use proximity-based location
- No screening out of sexual offenders
- DAppSAs more likely to be currently enrolled college students (compared to non DAppSAs)
- Male victims – percentage of DAppSA male victims was 2x more than rate of non DAppSA male victims
- DAppSA victims were significantly more likely to self-report mental health and chronic medical issues

Resource:

Valentine, J.L., Miles, L.W., Mella Hamblin, K., & Worthen Gibbons, A. (2023). Dating App Facilitated Sexual Assault: A Retrospective Review of Sexual Assault Medical Forensic Examiation Charts. Journal of Interpersonal Violence, 38(9-10), 6298-6322.

Use of Technology to Stalk: Responding to Victims

SPARC
STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Should victims just log off?

Safety Planning and Technology

Victims may consider:

- Secure passwords
- Hard-to-guess security questions
- Enable 2-factor authentication
- Use a second, safer device when/if possible
- Learn about settings and location-sharing defaults, set these intentionally
- Be mindful of smart device and social media usage

Safety Checks

- Android and Gmail users should use Google’s Security Checkup
- Apple users should update their phones and use Apple’s Safety Check

Gmail Safety Check

- Gmail account is connected to and controls the key safety elements of Android phones
- Gmail account is also the key to many important accounts for password reset
- Go to Security Checkup and review all tabs
  - Check access, sign-in, recovery, and sharing including email forwarding or linked accounts
- URL: https://myaccount.google.com/security-checkup

Apple Safety Check

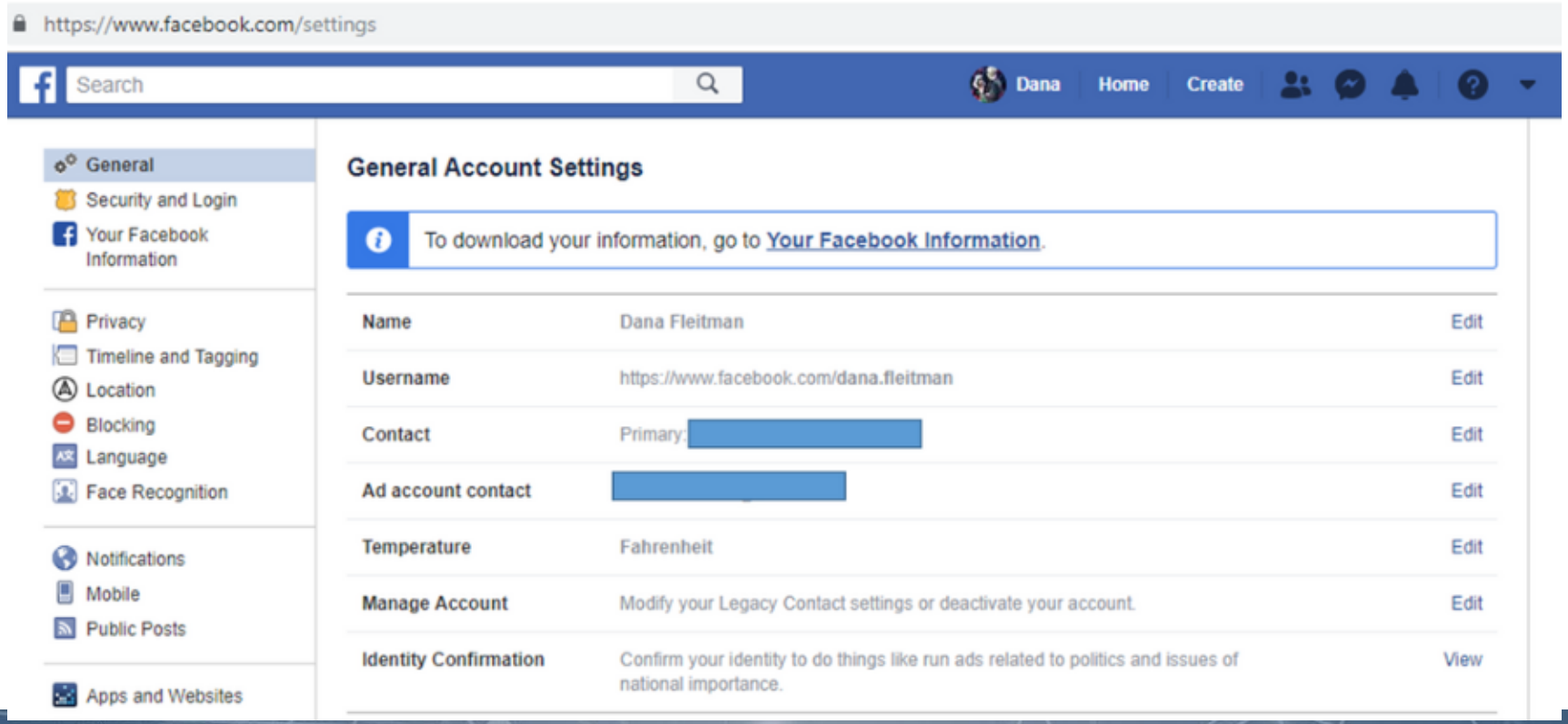
- Where?
  - Settings → Privacy and Security → Safety Check
- Why?
  - Location tracking, text messages, phone call history, emails, credit cards
  - Highest risk!

Documentation

- Screenshot or take photos of call log / text conversation
- Overlap screenshots / photos
- Capture time and date
- Take screenshot / photo of the contact info
- Consider apps like Tailor or StitchIt

Facebook Documentation

- Capture and save screenshots
- Some sites offer a "download your information" service in account settings



Technology & Stalking: Big Picture

- Believe victims. Offenders can misuse technology a variety of creative ways to access, contact, and monitor their victims.
- This technology is out there – and it's easy to use. Offenders don't have to be particularly "tech savvy" to terrorize victims through technology.
- Build knowledge on privacy/sharing settings across applications and devices. Sharing settings/defaults are often not intuitive.
- Ask specific questions about offender contact and knowledge. This can better help you collect evidence and safety plan.
- Consider both evidence preservation and victim safety. See if the victim has access to a safer device.
- Charge relevant technology-related crimes (when appropriate and applicable).

Just Tech

- Just Tech: Investigation and Prosecution of Online Abuse is a project of Aequitas and SPARC.
- Targeting prosecutors and law enforcement officers, Just Tech aims to increase the likelihood of positive case outcomes and victim experiences, as well as address the disproportionate impact of online abuse experienced by underserved communities.

NNEDV Tech Safety

- The NNEDV Tech Safety App contains information that can help someone identify technology-facilitated harassment, stalking, or abuse and includes tips on what can be done. Available in English and Spanish.
- URL: www.techsafety.org

For Victims

- Victim Connect
- URL: https://victimconnect.org/
- Victim Connect Resource Center provides confidential referrals for crime victims
- Phone: 855-484-2846 (855-4-victim)

Stalking Incident Log

- Date
- Time
- Description of incident (short)
- Location of incident (physical location, technology used, online platform)
- Witness names and contact info
- Evidence (photos, video, screenshots, items, etc.)
- Report (who it was made to – name, office/org, badge or identification number)

Wrap Up and Resources

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

Stalking Resources

- Stalking response checklists for organizations and campuses available online
- URL: www.StalkingAwareness.org

Campus Resources

- Resources for campus investigations and hearings
- Resources for stalking and Title IX
- URL: www.StalkingAwareness.org

Stalking Awareness Brochures

- Order stalking awareness brochures and posters for your community today!
- URL: https://www.stalkingawareness.org/know-it-name-it-stop-it/

SPARC Website

- URL: www.StalkingAwareness.org
- Available resources include:
  - Practitioner guides
  - Training modules
  - Victim resources
  - Webinar recordings
- Sign up for our newsletter
- Follow us on Facebook, Instagram, and Twitter
  - @FollowUsLegally

Contact Information – Kendra Eggleston

Kendra Eggleston, M.A.

Training & Campus Specialist

- Phone number: 202.642.0295
- Email: KEggleston@StalkingAwareness.org
- URL: www.StalkingAwareness.org
- @FollowUsLegally – Instagram, Facebook, X (Twitter)