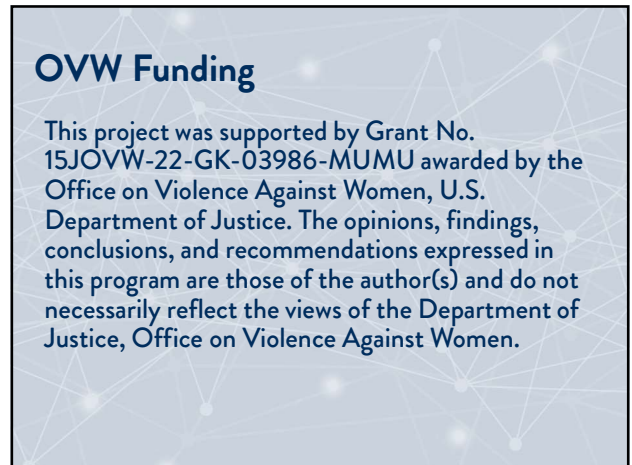




1



2



3



4



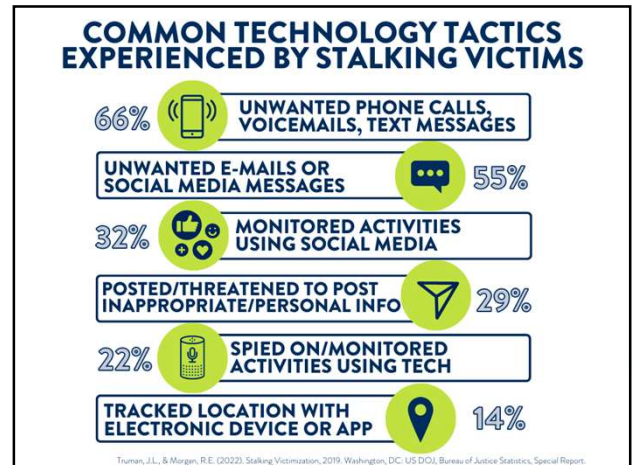
5



6

SURVEILLANCE - Smart home devices - Tracking software - Tracking devices - Monitoring online activity - Accessing online accounts - Cameras or audio/video recording devices	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
INTERFERENCE - Spreading rumors online - Doxing - Swatting - Posing as victim and creating harm - Posting private photos, videos, information online, real or fake - Using technology to encourage others to harm the victim	INTIMIDATION - Online threats - Blackmail - Sextortion - Threats to release private info, photos, or videos (real or fake) - Threats to interfere with property, employment, finances, accounts

7



8



9

Tracking Location

STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

10

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

11

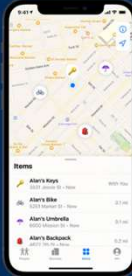
STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

12



13

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

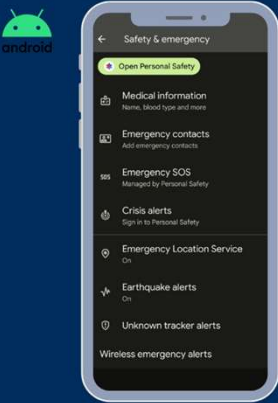
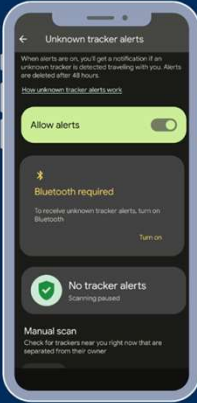
14

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

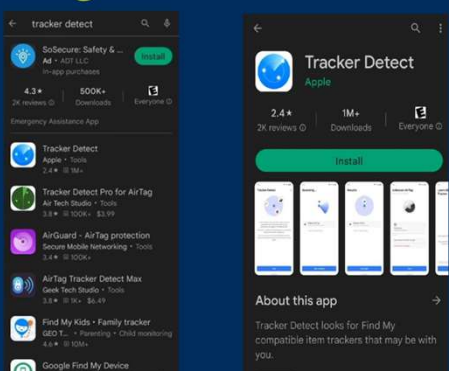


15

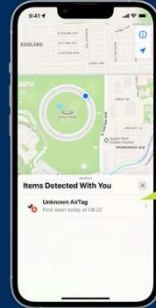
16

AirTag Alert: Android



17

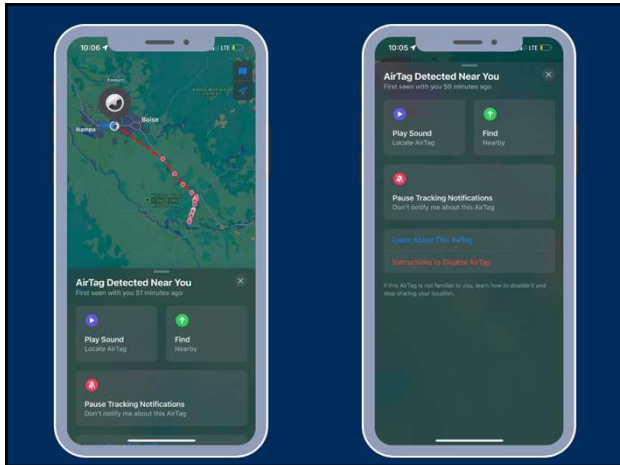
AirTag Alert: Apple



Items Detected With You

Unknown AirTag
First seen today at 08:22

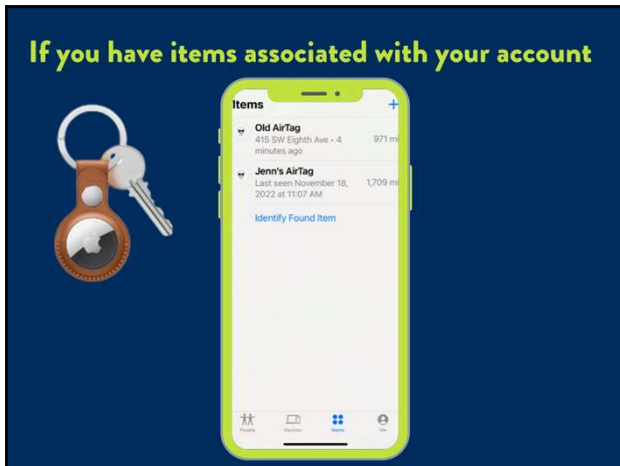
18



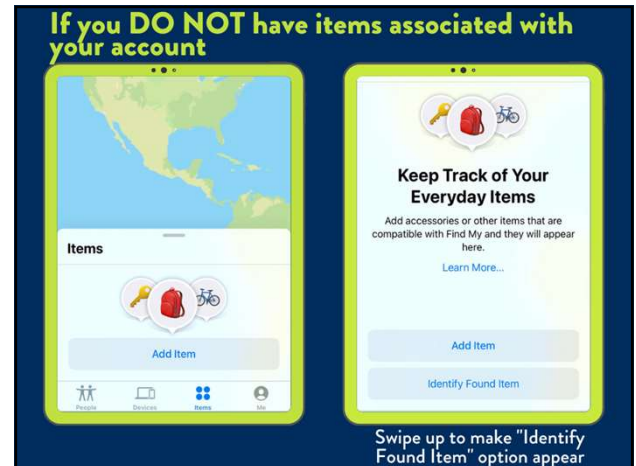
19



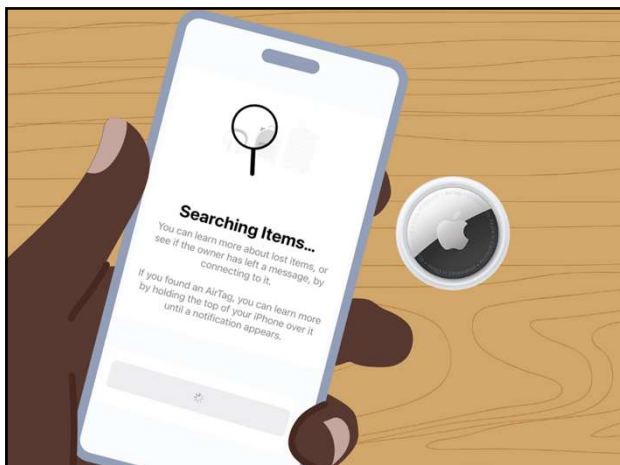
20



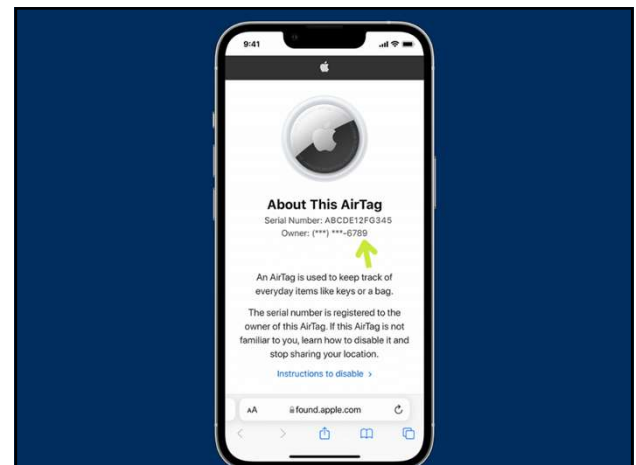
21



22



23



24



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

25

Evidence with AirTags

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

SPARC STRATEGIC POLICE ANALYSIS, RESEARCH & CONSULTING

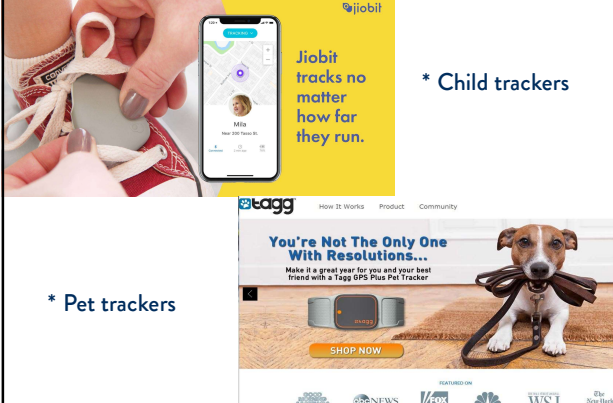
26

Global Positioning System (GPS) Devices



SPARC

27



SPARC

28



29



30

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

31

Percentage of People Checking In or Sharing Their Location By Platform and Privacy Settings

	Private	Public		Private	Public
Facebook	57.1%	42.9%	Snapchat	60.9%	39.1%
Instagram	43.5%	56.5%	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.

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

32

Spoofing

33

How can you remain anonymous when you call someone? The best way is by using SpoofCard. With SpoofCard you can change your CallerID to

34

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."

35

SPOOFTEL
THE WORLD'S LEADER IN CALLER ID SPOOFING

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 real, it involves more than a changed number. At SpoofTel, our services come along with a wider range of options.

Your Number
Enter the number you are calling from

Voice Pitch
Adjust the pitch of your voice

Destination Number
Enter the number you would like to call

Soundboard
Name

Spoof Number

DLPERN

Copyright © 2014 - 2020 SpoofTel Ltd. All Rights Reserved.

36

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

37

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

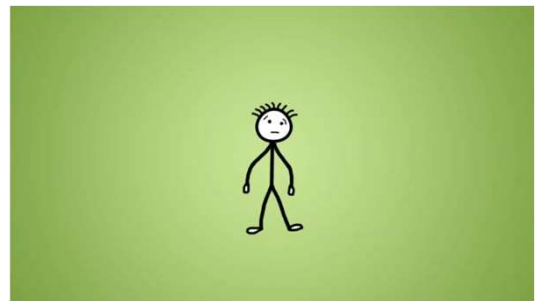
38

Stalkerware

SPARC STALKING PREVENTION AWARENESS AND RESOURCE CENTER

39

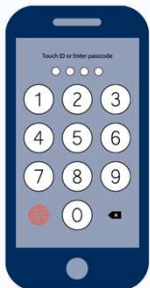
Cell Phone Spyware



SPARC

40

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."

41

What is Stalkerware?



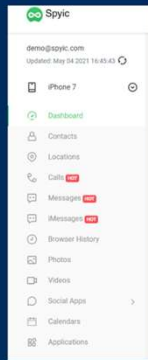
- Commercially available software used for spying
- Made for individual use
- Typically hides itself from the list of installed programs and does not display any activity notifications

COALITION AGAINST STALKERWARE

42

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



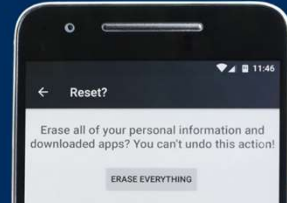
COALITION AGAINST STALKERWARE

43

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



COALITION AGAINST STALKERWARE

44

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

45

Public Data

SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

46

Geotagging



SPARC STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER

47

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

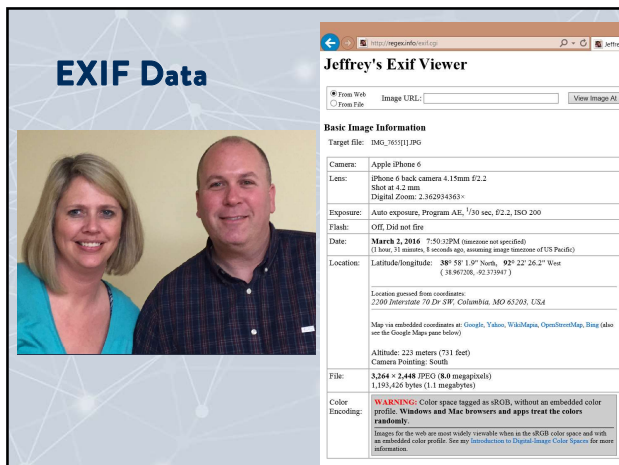
Exif Wizard
By homedatasheet.com,
Open iTunes to buy and down



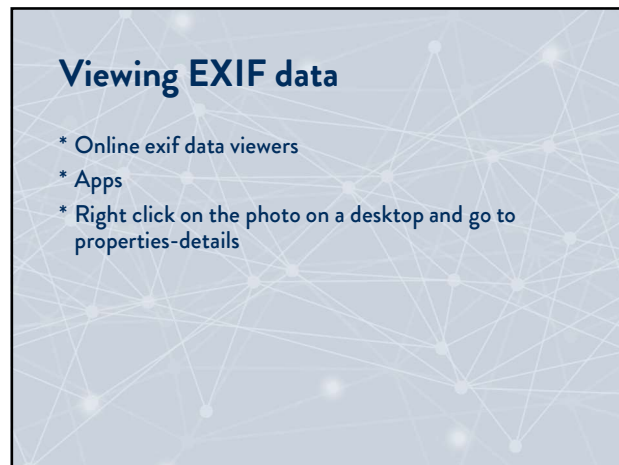
View in iTunes

SPARC

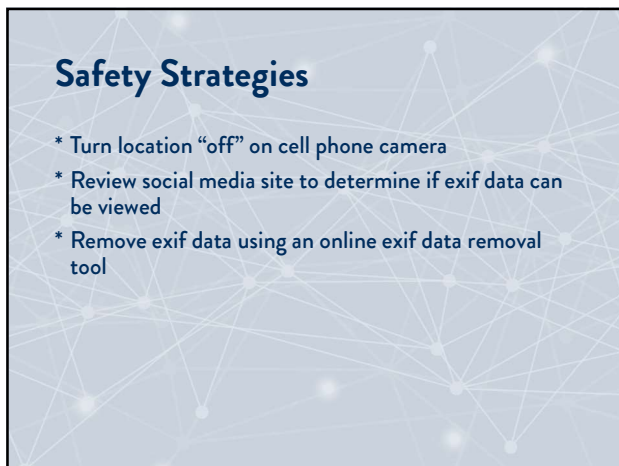
48



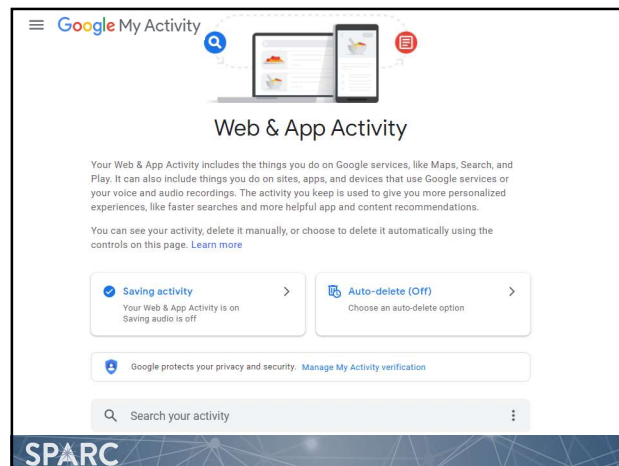
49



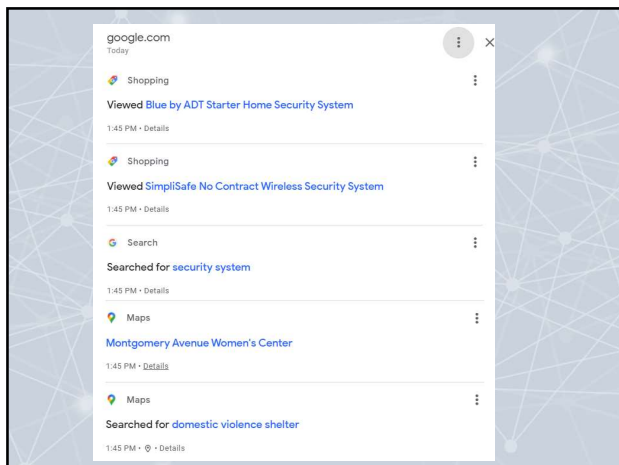
50



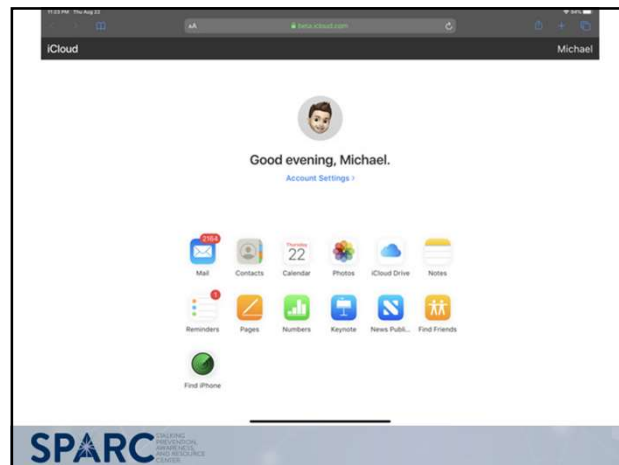
51



52



53



54

Find Yourself...

- * FastPeopleSearch.com
- * TruePeopleSearch.com
- * PeopleSearchNow.com

55

Non-Consensual Distribution of Intimate Images

SPARC STALKING, PREVENTION, AWARENESS, AND RESOURCE CENTER

56

16% OF VICTIMS 18-24 YEARS OLD

REPORT THAT THE STALKER SHARED NUDE, SEMI-NUDE, AND/OR SEXUALLY EXPLICIT PHOTOS OR VIDEOS OF THEM

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

57

New AI deepfake app creates nude images of women in seconds

/ The resulting fakes could be used to shame, harass, and intimidate their targets

Artificial Intelligence X-Ray App

Download For Free or Try Online

By JAMES VINCENT
Jun 27, 2019, 6:23 AM EDT | 0 Comments | 0 New

The Deepfake app creates AI fakes at the click of a button.

SPARC STALKING, PREVENTION, AWARENESS, AND RESOURCE CENTER

58

Nonconsensual Image Resources

#CCRI Image Abuse Helpline: 1-844-878-2274
Cyber Civil Rights Initiative CyberCivilRights.org

StopNCII.org
Stop Non-Consensual Intimate Image Abuse

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

DMCA DEFENDER
DMCADefender.com



59

Technology-Facilitated Stalking and Sexual Assault

SPARC STALKING, PREVENTION, AWARENESS, AND RESOURCE CENTER

60

Sexual Assault, Stalking, & 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

61

DENVER 04/07/2010 05:12 am ET | Updated Dec 06, 2017

Jebidiah Stipe, Wyoming Marine, Solicited Ex-Girlfriend's Rape And Assault On Craigslist

Details emerge in Web rape case

California Marine also tried to solicit rape of ex-wife, authorities say

By WILLIAM BROWNING - Star-Tribune staff writer Feb 5, 2010

Judge gives man 60 years in Craigslist rape case

SPARC SEXUAL ASSAULT PREVENTION, AWARENESS, AND RESOURCE CENTER

62

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 SAs than acquaintance SAs
 - 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."

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 Examination Charts. *Journal of Interpersonal Violence*, 38(9-10), 6298-6322.

63

Dating App Concerns



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

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 Examination Charts. *Journal of Interpersonal Violence*, 38(9-10), 6298-6322.

64

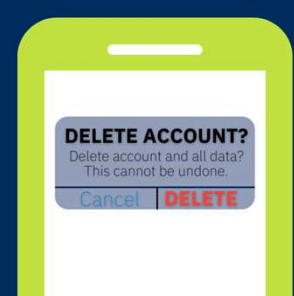
Use of Technology to Stalk

Responding to Victims

SPARC SEXUAL ASSAULT PREVENTION, AWARENESS, AND RESOURCE CENTER

65

Should victims just log off?



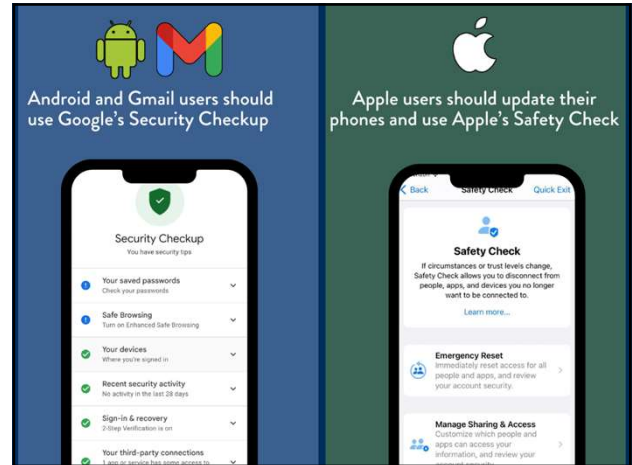
66

Safety Planning and Technology

Victims may consider:

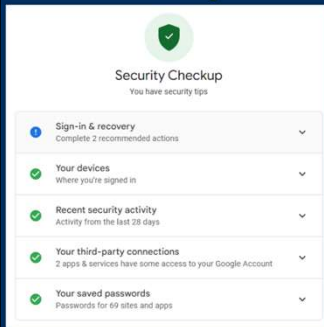
- Secure passwords
- Hard-to-guess security questions
- Enable 2-factor authentication
- Use a second, safer device when/if possible
- Learn about settings and location-sharing defaults, set these intentionally
- Be mindful of smart device and social media usage

67



68

Gmail Safety Check



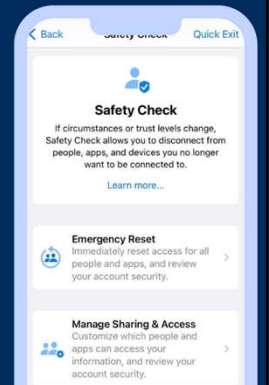
[MyAccount/Google.com/security-checkup](https://myaccount.google.com/security-checkup)

- Gmail account is connected to and controls key safety elements of Android phones
- Gmail account is also key to many important accounts for password reset
- Go to Security Checkup and review all tabs
 - Check access, sign-in, recovery, and sharing - including e-mail forwarding or linked accounts

69

Apple Safety Check

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



70

Documentation

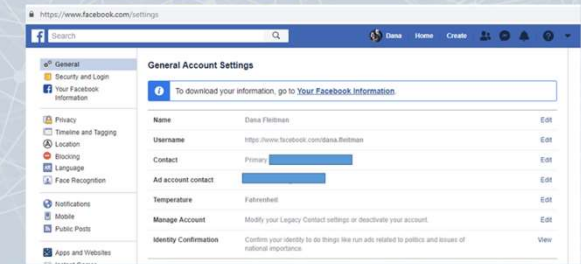
- * Screenshot or take photos of call log / text conversation
- * Overlap screenshots / photos
- * Capture time and date
- * Take screenshot / photo of the contact info
- * Consider apps like Tailor or Stitchlt



71

Facebook Documentation

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



72

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).

73

JUST TECH



INVESTIGATION & PROSECUTION OF ONLINE ABUSE

AEQUITAS 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.

74

NNEDV Tech Safety

Tech Safety

Welcome to the Tech Safety App. This app contains information that can help someone identify technology-facilitated harassment, stalking, or abuse and includes tips on what can be done.

Download on the App Store | Get it on Google play

SPARC

75

For Victims

Victim Connect

resource center

Confidential referrals for crime victims 855-4-VICTIM

76

STALKING INCIDENT LOG

Date	Time	Description of Incident	Location of Incident	Witness Name(s) (Attach Address and Phone #)	Police Called (Report #)	Officer Name (Badge #)

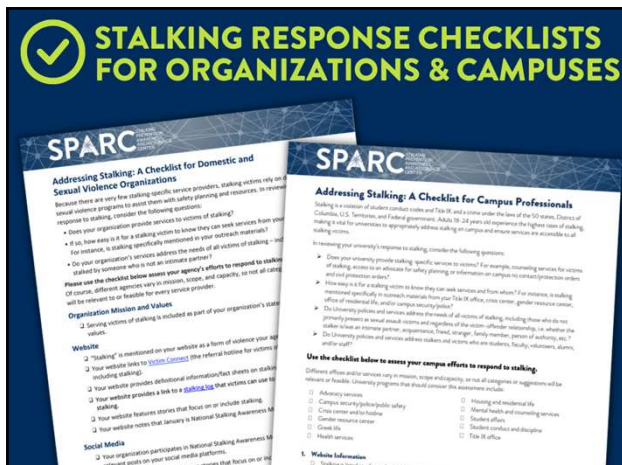
SPARC

77

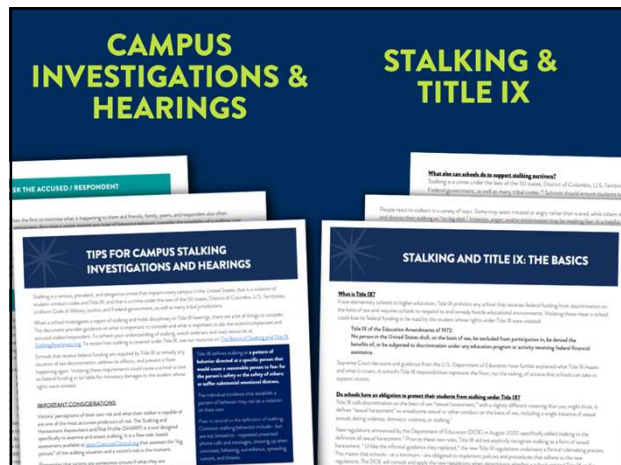
Wrap Up & Resources

SPARC

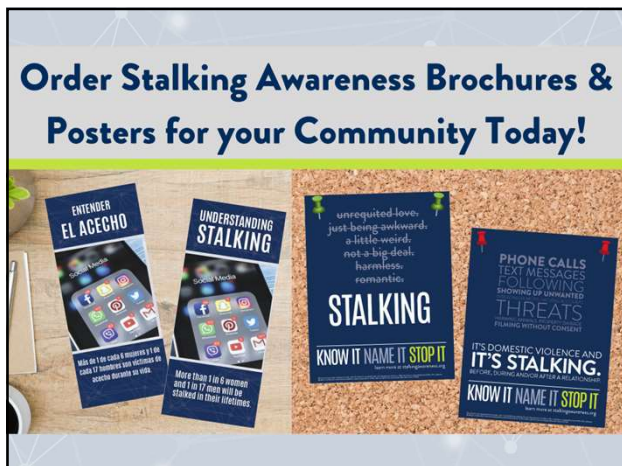
78



79



80



81



82



83