

TECHNOLOGY SAFETY SERIES: Abuse Using Technology

BY FLORENCE VICIL

AS A COURTESY TO DOMESTIC VIOLENCE VICTIM ADVOCATES IN FLORIDA



1



FLORENCE'S BIO



- Former Orlando PD officer
- Guardian ad Litem, Osceola County
- Computer Programmer, B.S., M.S.
- Member, Code for Orlando, Code for America Brigade
 - <http://www.codefororlando.com/>
 - <http://staysafeorlando.com/>
- Member, STEADI [Sex Traffic/Exploitation/Abuse Dismantling Initiative]
 - <https://www.meetup.com/STEADI-Sex-Traffic-Exploit-Abuse-Dismantling-initiative/>

<https://www.linkedin.com/in/vicilanaya/>

vicilanaya@gmail.com

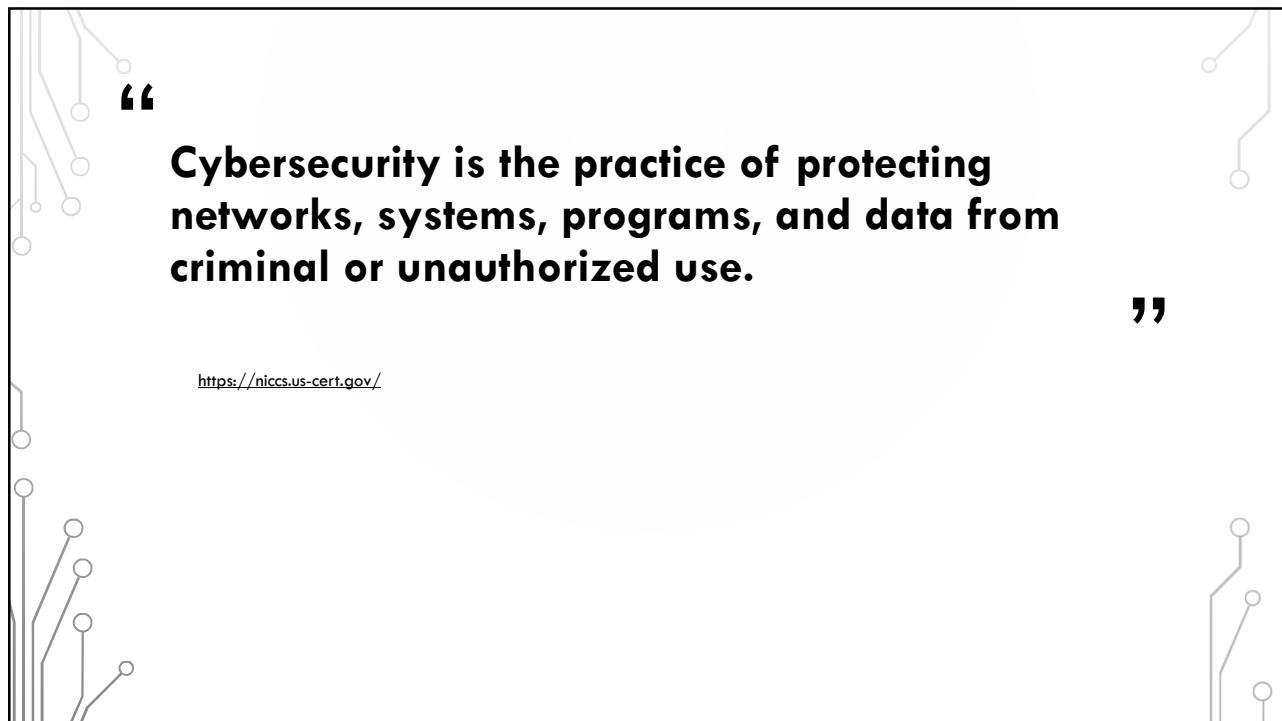
2



ABUSE USING TECHNOLOGY

"TECHNOLOGY-ENABLED COERCIVE CONTROL" IN INTIMATE PARTNER VIOLENCE

3



“

Cybersecurity is the practice of protecting networks, systems, programs, and data from criminal or unauthorized use.

”

<https://niccs.us-cert.gov/>

4

TECHNOLOGY ABUSE – WHO?

- Abusers:
 - Current or former partners
 - Strangers
- Victims:
 - Any person and/or their children, family or friends



5

TECHNOLOGY ABUSE – CRIMES: DEFINITIONS

- **Credible threat** = a verbal or nonverbal threat, or a combination of the two, including threats delivered by electronic communication or implied by a pattern of conduct, which places the person who is the target of the threat in reasonable fear for his or her safety or the safety of his or her family members or individuals closely associated with the person, and which is made with the apparent ability to carry out the threat to cause such harm
- It is not necessary to prove that the person making the threat had the intent to actually carry out the threat.
- The present incarceration of the person making the threat is not a bar to prosecution under this section.

6

TECHNOLOGY ABUSE – CRIMES: DEFINITIONS

- **Harassment** = to engage in a course of conduct directed at a specific person which causes substantial emotional distress to that person and serves no legitimate purpose (§784.048(1)a)
- **Course of conduct** = means a pattern of conduct composed of a series of acts over a period of time, however short, which evidences a continuity of purpose (§784.048(1)b)
- **Cyberstalking** = to cause substantial emotional distress to a person and serving no legitimate purpose by:
 - Engaging in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person; or
 - Accessing, or attempting to access, the online accounts or Internet-connected home electronic systems of another person without that person's permission (§784.048(1)d)

§ = Florida Statutes section

7

TECHNOLOGY ABUSE – CRIMES: MISDEMEANORS

- **Stalking** = to willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person (§784.048(2))
- **Sexual cyberharassment** = to publish a sexually explicit image of another to Internet websites or to disseminate such an image through electronic means without the depicted person's consent, contrary to the depicted person's reasonable expectation of privacy, for no legitimate purpose, with the intent of causing substantial emotional distress to the depicted person (§784.049(2)(c))



8

TECHNOLOGY ABUSE – CRIMES: FELONIES

- **Sexual cyberharassment**
 - If prior conviction (§784.049(3)(b))
- **Aggravated stalking** = to willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person and makes a credible threat to that person (§784.048(3))
- **Aggravated stalking**
 - If victim is child under 16 yo (§784.048(5))
 - If after injunction (§784.048(4)), credible threat not required
 - If after sentencing for certain sexual crimes (§784.048(7))

9

TECHNOLOGY ABUSE – FL COMPUTER CRIMES ACT (§815)

- Felonies
 - Offenses against intellectual property
 - Disclosure of trade secrets (§812.081)
 - Unauthorized access, disruption of data/service/medical equipment, destruction of equipment, introduction of computer contaminant, audio or video surveillance, fraud, endangering human life
- Misdemeanors
 - Modifying equipment



10

TECHNOLOGY ABUSE – OTHER CRIMES

- Tampering with or harassing a witness/victim/informant (§914.22)
 - Hinder communication with LEO
- Tampering with or fabricating physical evidence (§918.13)
- Written threats to kill or do bodily injury (§836.10)
- Obscene or harassing phone calls (§365.16)
 - Cause phone to ring repeatedly

11

TECHNOLOGY ABUSE – HOW?

- Social media, text messages, email
- Computer activities, tablets
- Online accounts (phone, bank, etc.)
- Phone apps/features, phone land line
- Spoofing (caller ID, replyTo email)
- GPS tracking
- Gathering online data
- Posting abusive content online
 - Nonconsensual pornography (Revenge Porn)
 - Sextortion
- Toys/gifts with hidden “spying” technology
 - Cameras, microphones, GPS
- Smart/connected/wearable devices, IoT
 - Roadside assistance/safe driver service

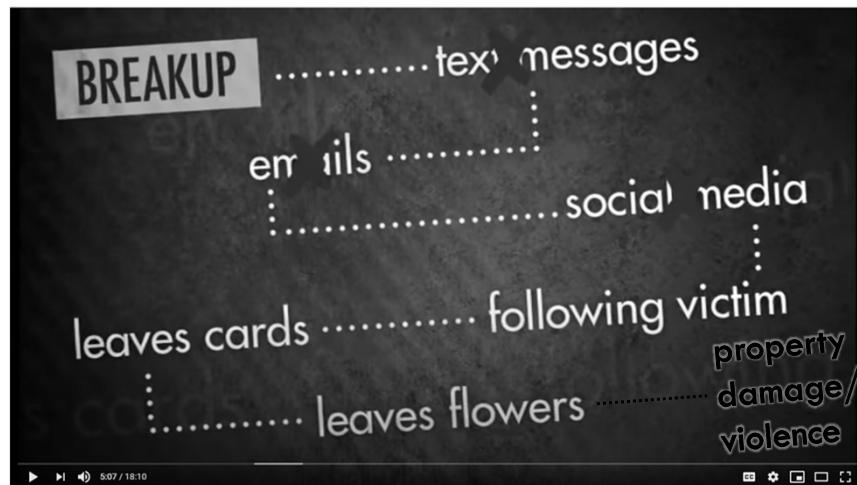
12

TECHNOLOGY ABUSE – HOW?

- Assistive technology/devices
 - Smart home assistants
 - Environmental control devices
 - Personal emergency response systems
 - Adaptive tools
 - Mobility aids
 - Communication aids

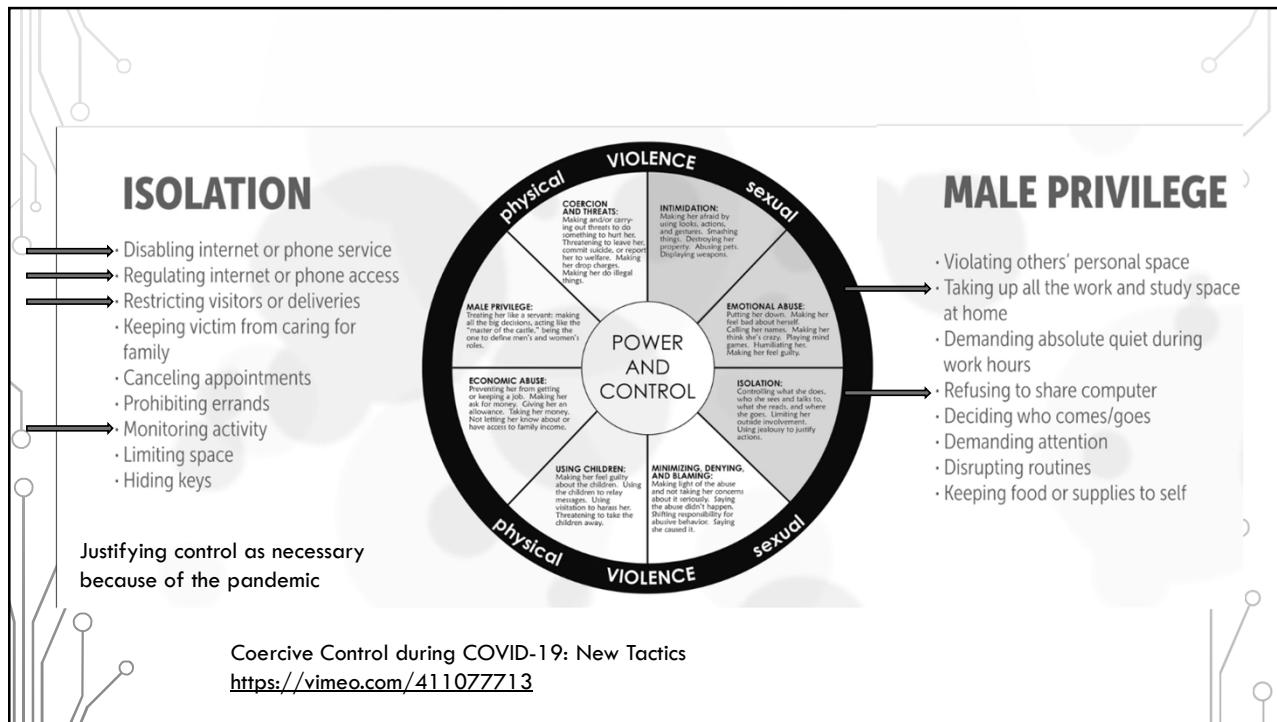


13

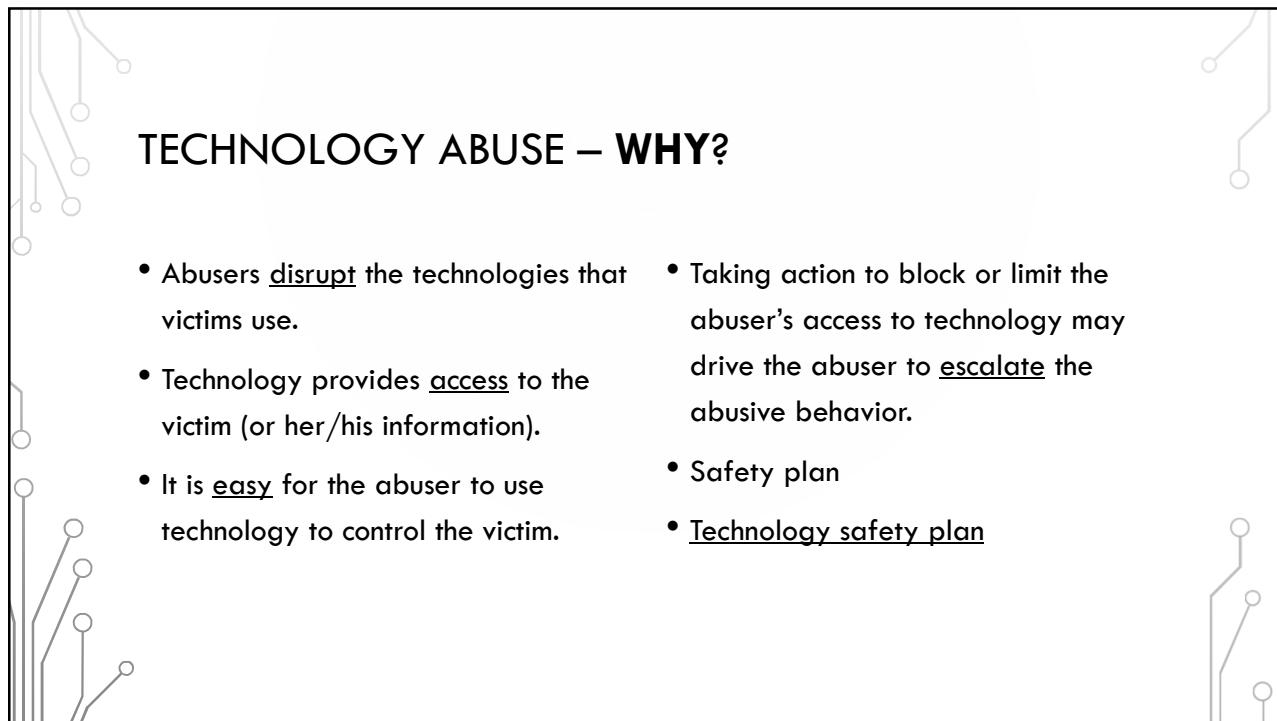


Connecting the Dots: Recognizing and Responding to Stalking
<http://www.evawintl.org/Library/Detail.aspx?ItemID=659>

14



15



16

TECHNOLOGY ABUSE – ASSESS THE SITUATION

- **What's happening?**

- Does it seem like the abuser knows too much about the victim?
- What technologies are being affected?
- How is the abuser gaining access to the victim's technologies?

- **Can the victim mitigate the situation?**

- Does the victim have the resources necessary?
- Is the victim tech savvy enough?
- Is there a current safety plan?
- Can the safety plan be adapted?
- How can the victim avoid family and friends compromising the safety plan?



17

THE PLAN

18

TECHNOLOGY ABUSE – WHAT TO DO?

- **Preserve evidence**

- Screenshot/record video/audio
 - Messages/emails/voicemails (visual)
 - Documents/pictures/videos
 - Call logs/transient evidence
- Send evidence to secure repository
- Print evidence
- Backup everything in separate storage
- Google Alerts

- **Document the abuse with an incident log**

- Record details of every abuse incident
- Dates, places (tech), witnesses, evidence
- Note beginning and end of behaviors
- Change in frequency of behaviors
- Escalation of behaviors
- Actions victim has taken to mitigate the abuser's behaviors

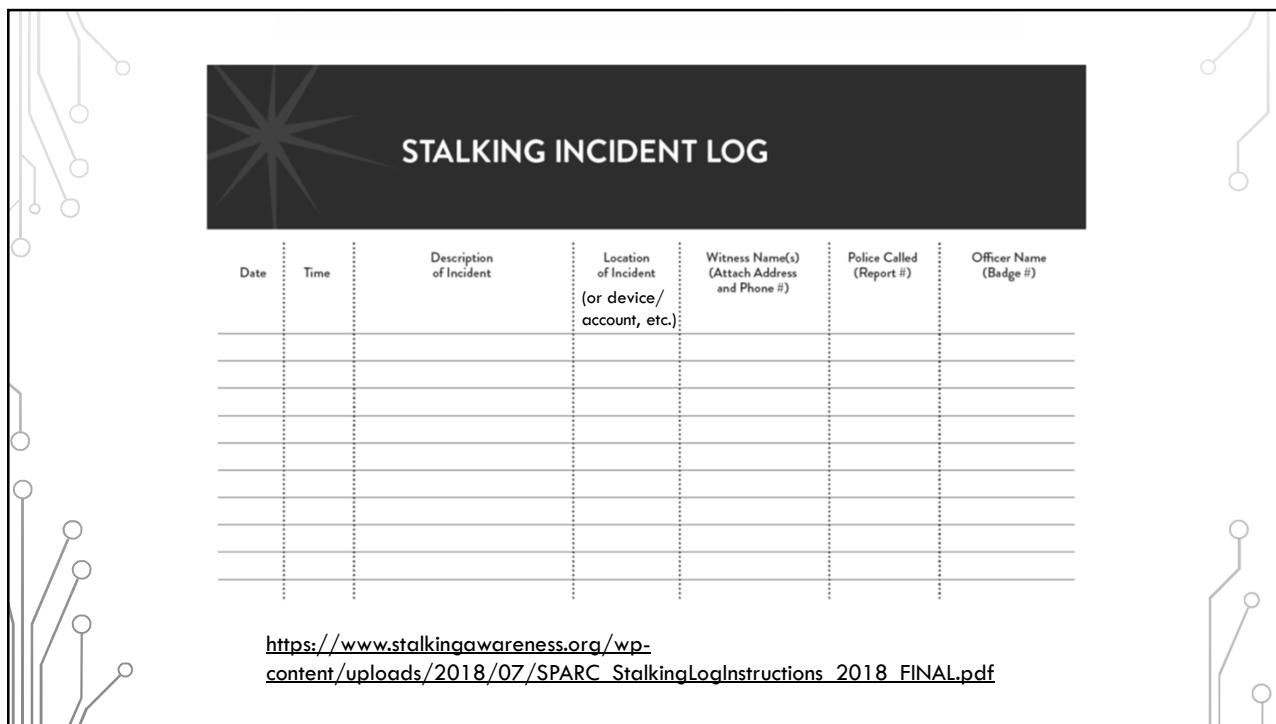
19

TECHNOLOGY ABUSE – SAMPLE LOGS

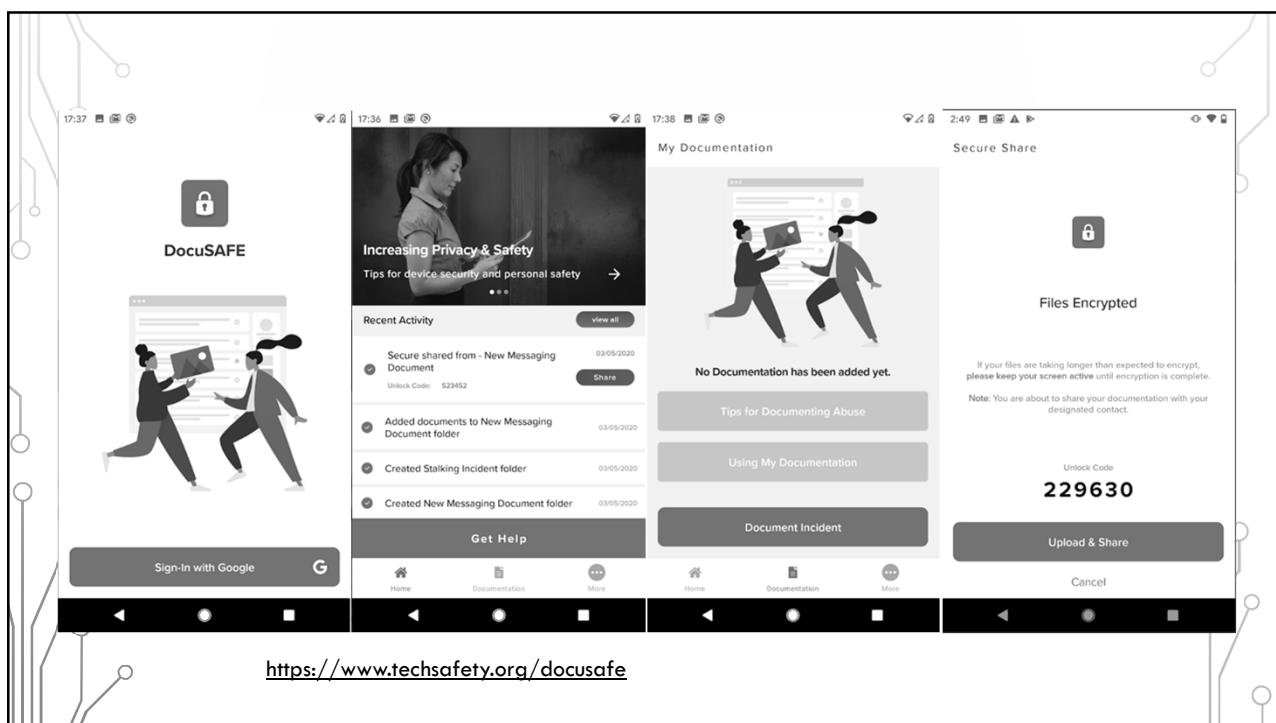
Information About the Abuser		Description of the Abuse
Name of the person abusing or stalking you.		Date: _____ Time: _____
Relationship of that person to you (if relevant).		Describe the event:
Contact information of that person		
Home address	Work address	
Phone number(s)	Email address(es)	Type of technology involved:
Online account(s), including screen name & type of online account (facebook, etc.)		Were there any witnesses? What are their names?
Other information about the abuser (that might be relevant)		
		Documentation If you were able to document the abuse, what type of documentation do you have?
		Other Information Did you report it to the police? If so, what is the report number and officer name?
		Did you go to the hospital/see a doctor? If so, what was the hospital/doctor name?

<https://www.techsafety.org/documentationtips>

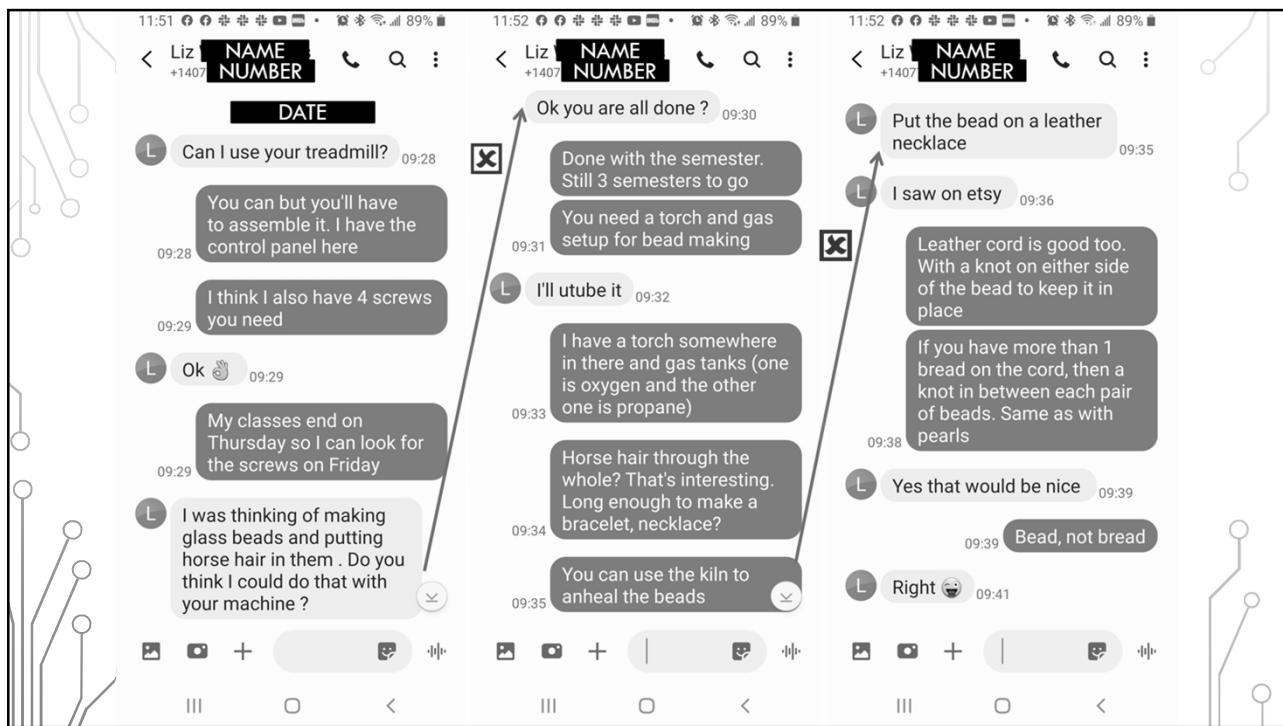
20



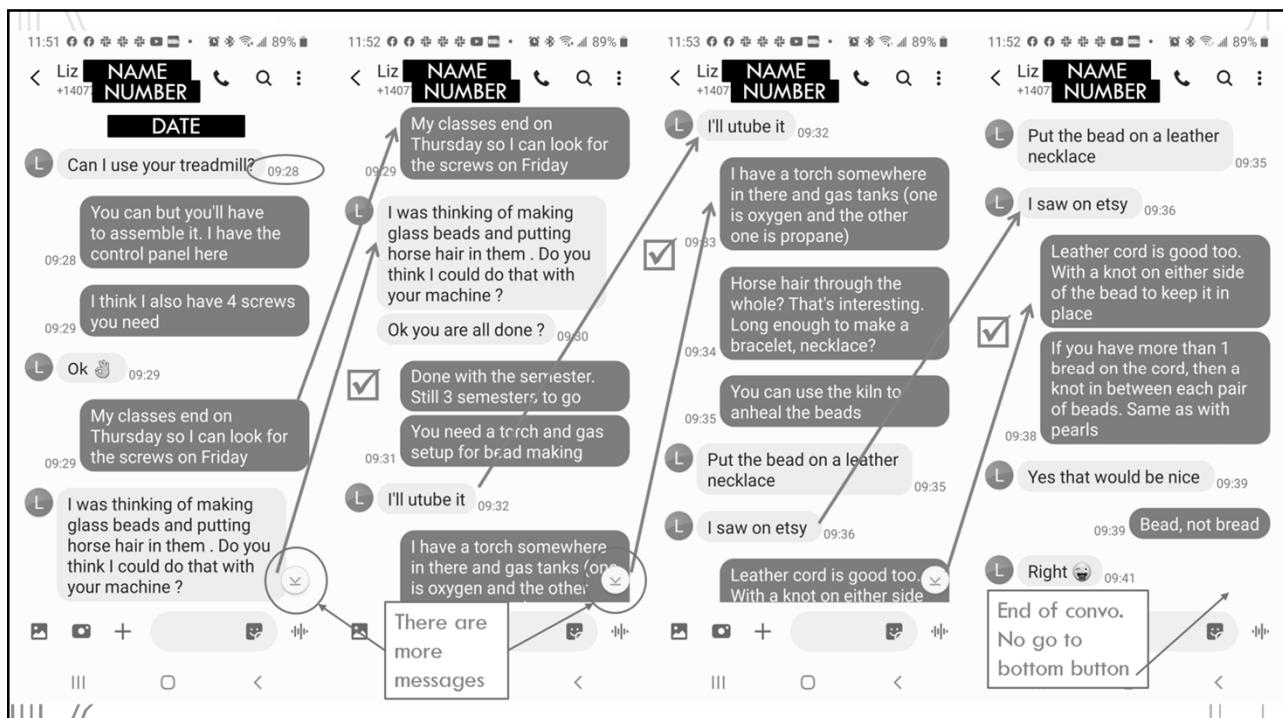
21



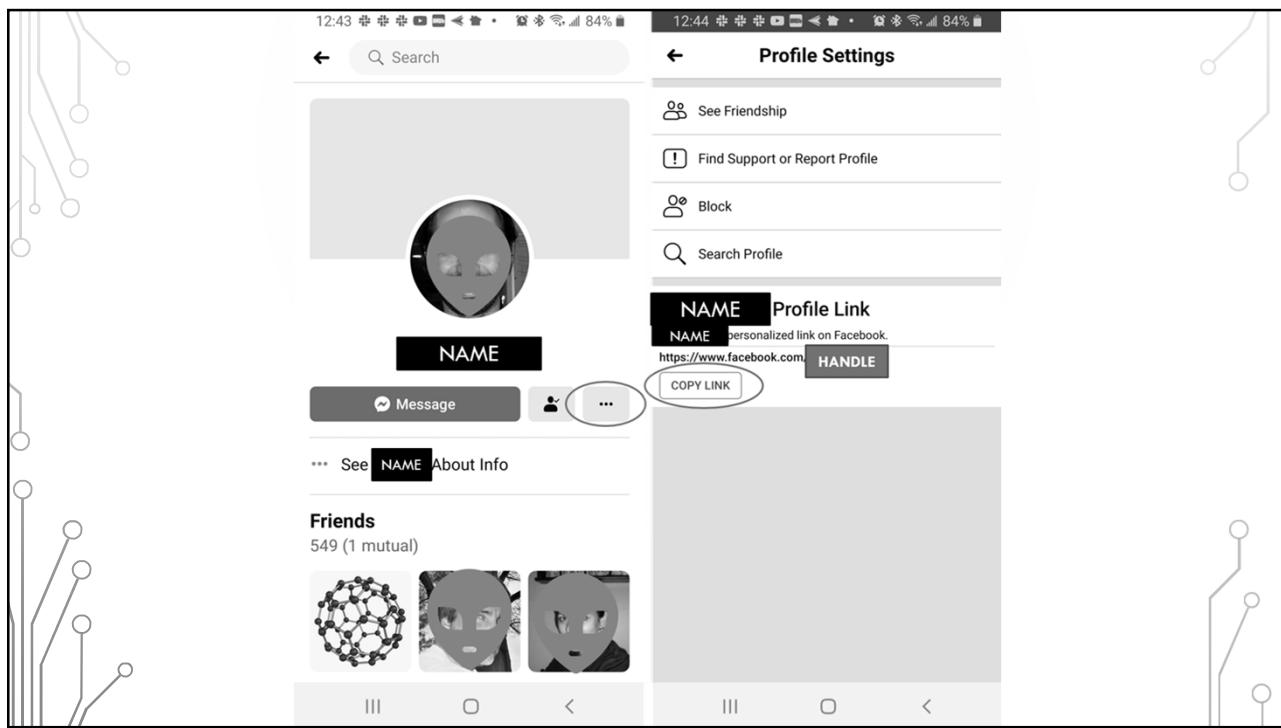
22



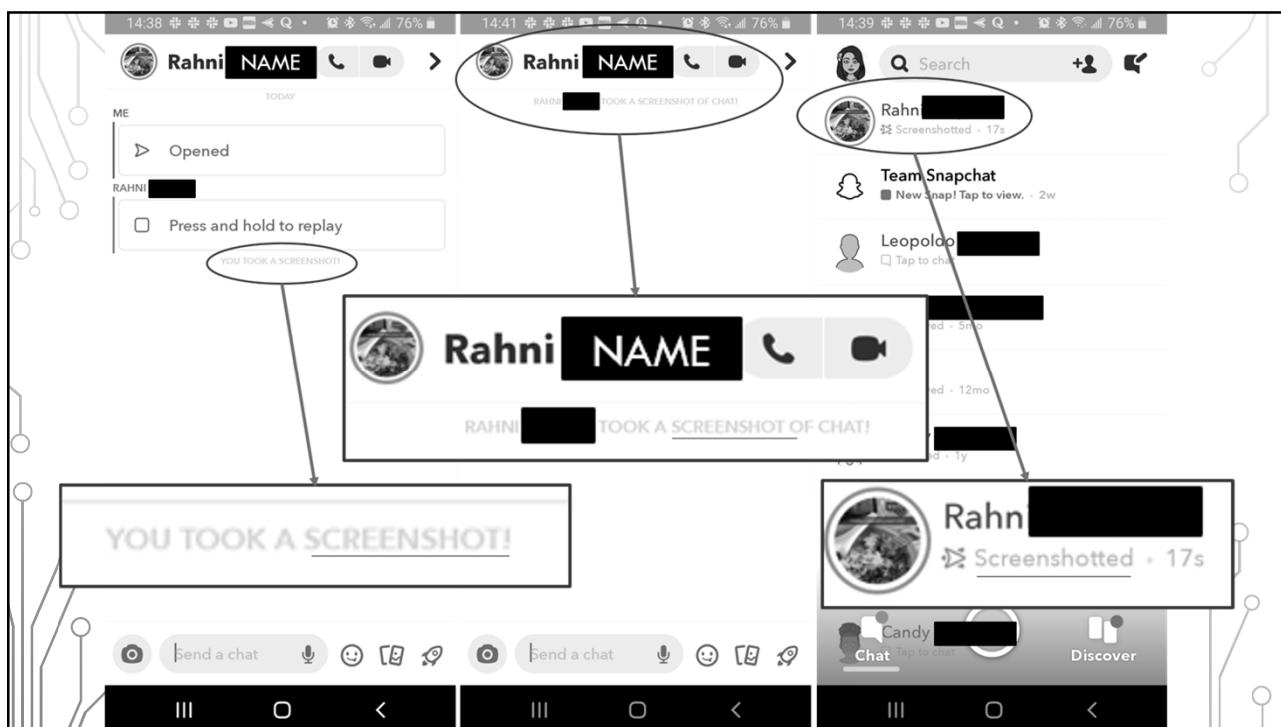
23



24



25



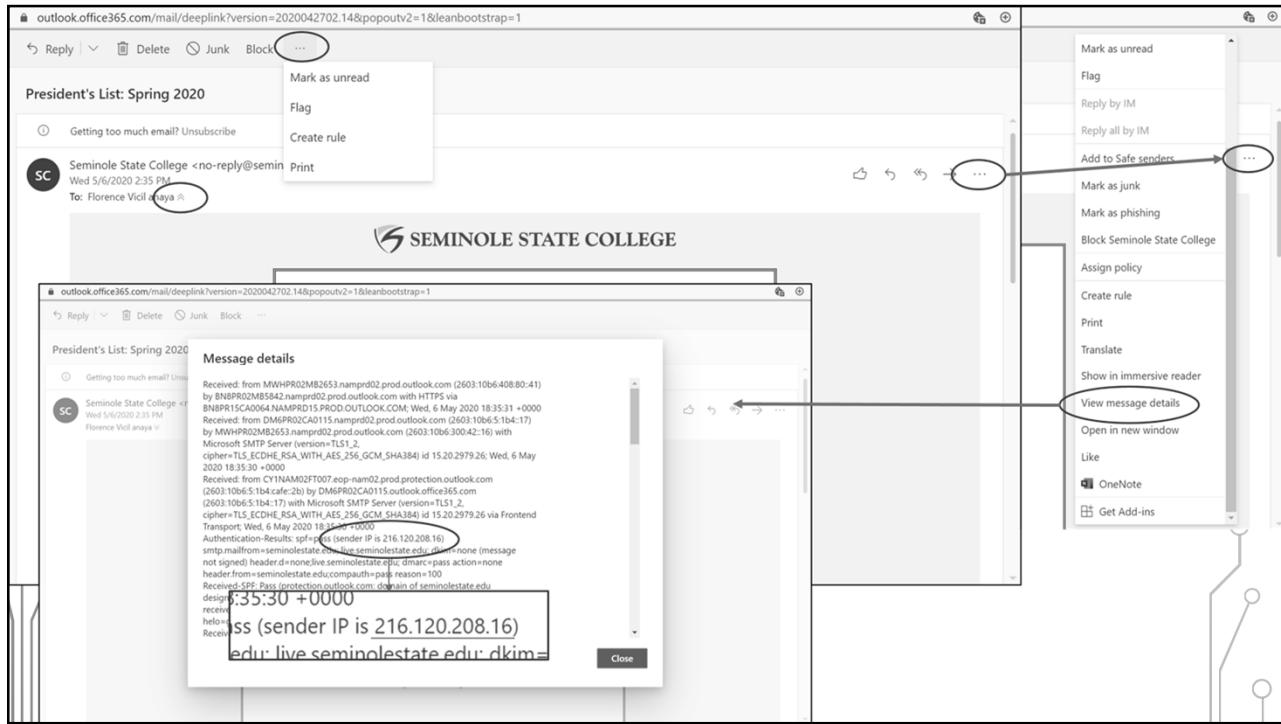
26



27



28



29

TECHNOLOGY ABUSE – WHAT TO DO?

- Practice digital hygiene
 - Decrease digital footprint
 - Use good password habits
 - Password manager
 - Keyloggers
 - Use multi-factor authentication
 - Use privacy settings
 - Always log out
 - Use webcam cover

30

TECHNOLOGY ABUSE – WHAT TO DO?

- Avoid malware

- Keep software up to date
- Use security software



- Limit device communication/location

- Disable

- WiFi/Bluetooth
- Peripherals/microphone
- GPS location/geo-tagging of media
 - Metadata = data about data
- Notifications



- Some messages cannot be deleted

- Replace or duplicate devices/accounts/log in information

- Devices you trust
- Devices you don't trust

- Keep old devices/accounts

- To not alert abuser of the changes
- To collect evidence

31

Device disappears
and reappears

Increase in
data usage

Unusual phone
behavior

Clues that stalking apps might be on your phone:



Abuser has
physical access
to your phone



Abuser knows
specific info
about you



Phone's
battery
drains faster



Unexplained
charges
on bill

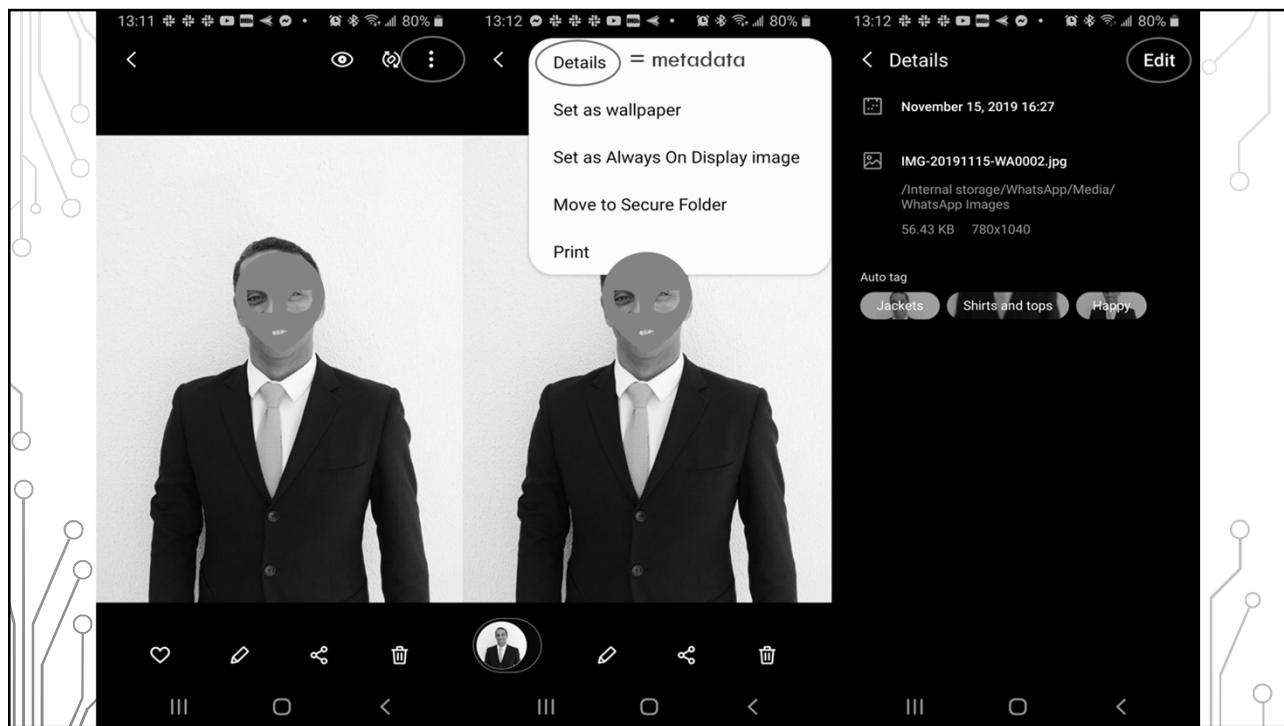


Trouble
turning off
phone

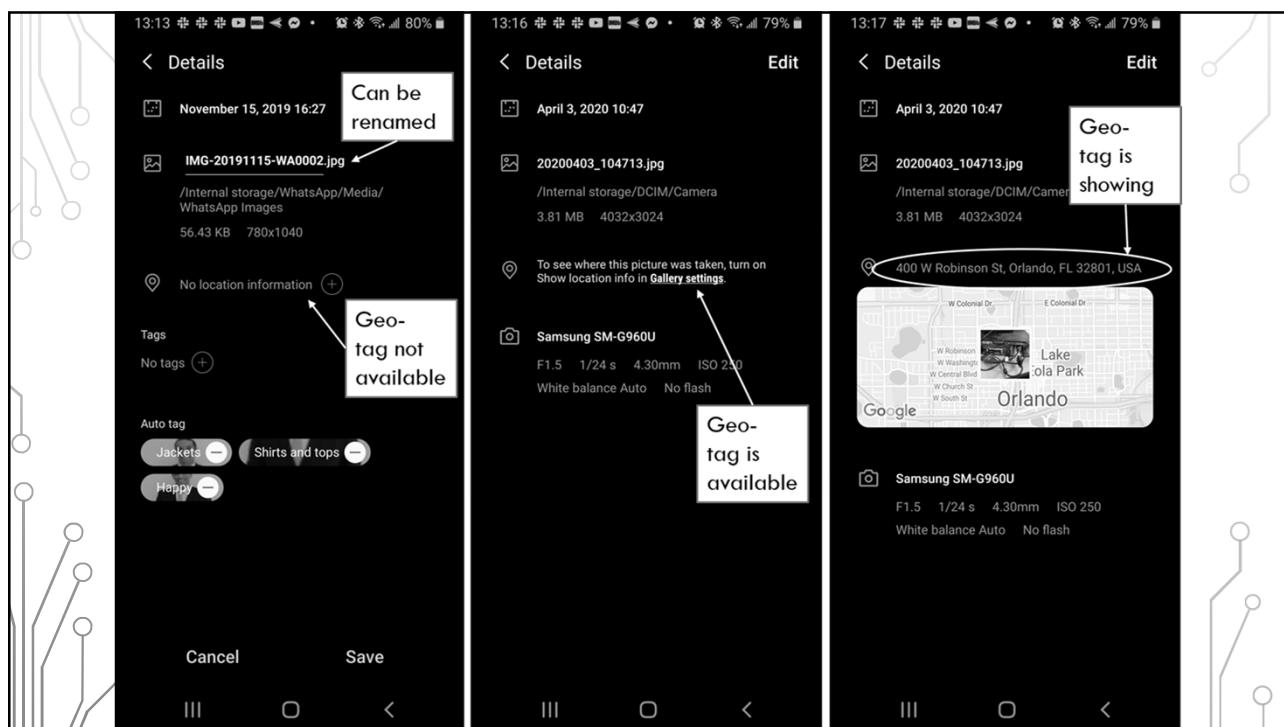


<http://www.stopstalkerware.org/>

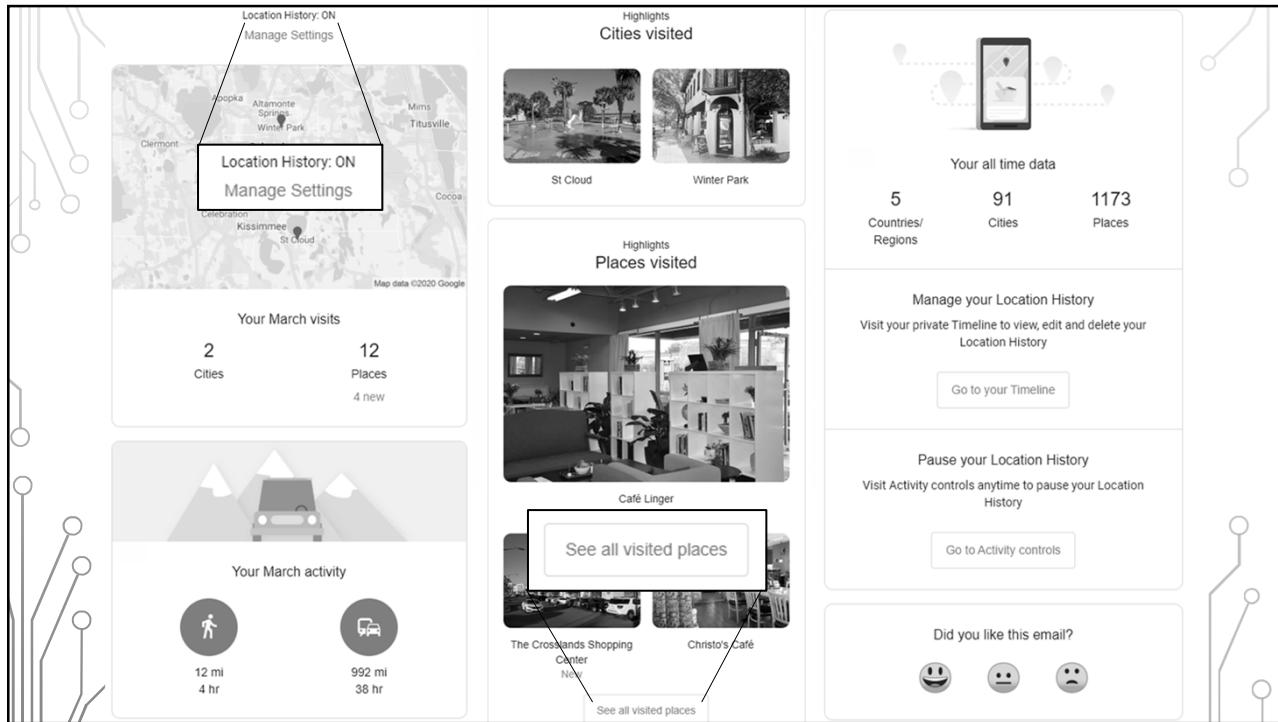
32



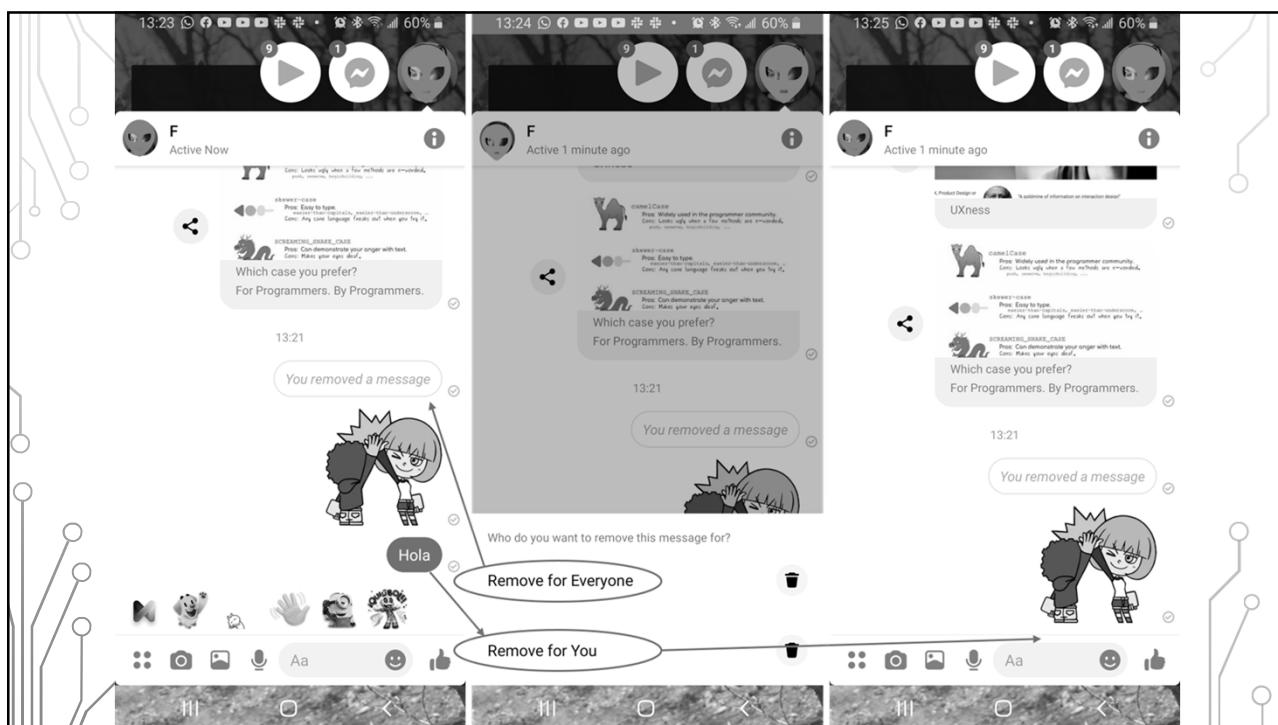
33



34



35



36

TECHNOLOGY ABUSE – WHAT TO DO?

- **Restrict access to your information**

- Freeze credit/accounts
 - <https://www.annualcreditreport.com>
 - <http://www.nctue.com/>
 - <https://www.innovis.com/>
 - <https://www.chexsystems.com/>
- Florida Attorney General's Address Confidentiality Program
 - <http://www.fcpti.com/fcpti.nsf/pages/AddressConfidentialityProgram>

- Request family violence indicators be placed on records to trigger nondisclosure
 - §61.1825(3)(a) State Case Registry
- Request exemption from public records
 - §119.071(2)(j)1 General exemptions from inspection or copying of public records

37

TECHNOLOGY ABUSE – WHAT TO DO?

- **Limit the information you share**

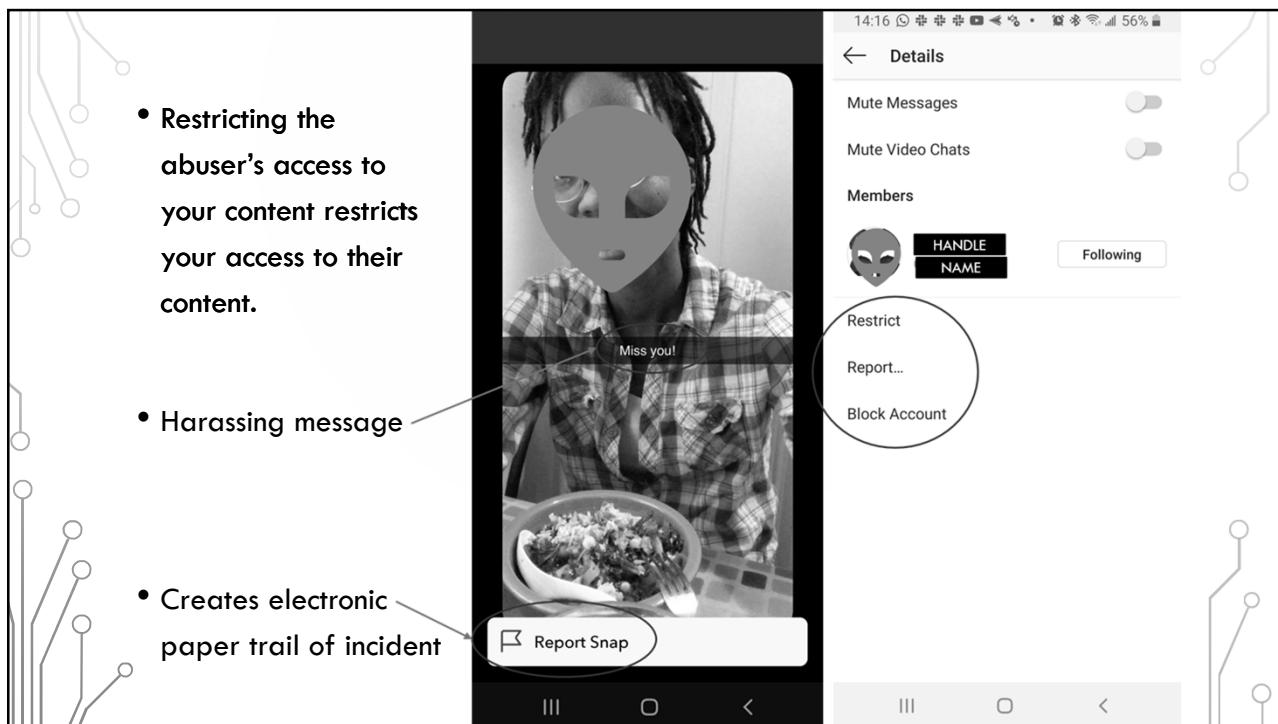
- Do not share accounts with the abuser
- Opt out of data collection (third-party tracking)
- Disable password saving in browsers/apps
- Do not share contact lists to see if your contacts are using the same service/network
- Make online profiles non-searchable

- **Report the abuse**

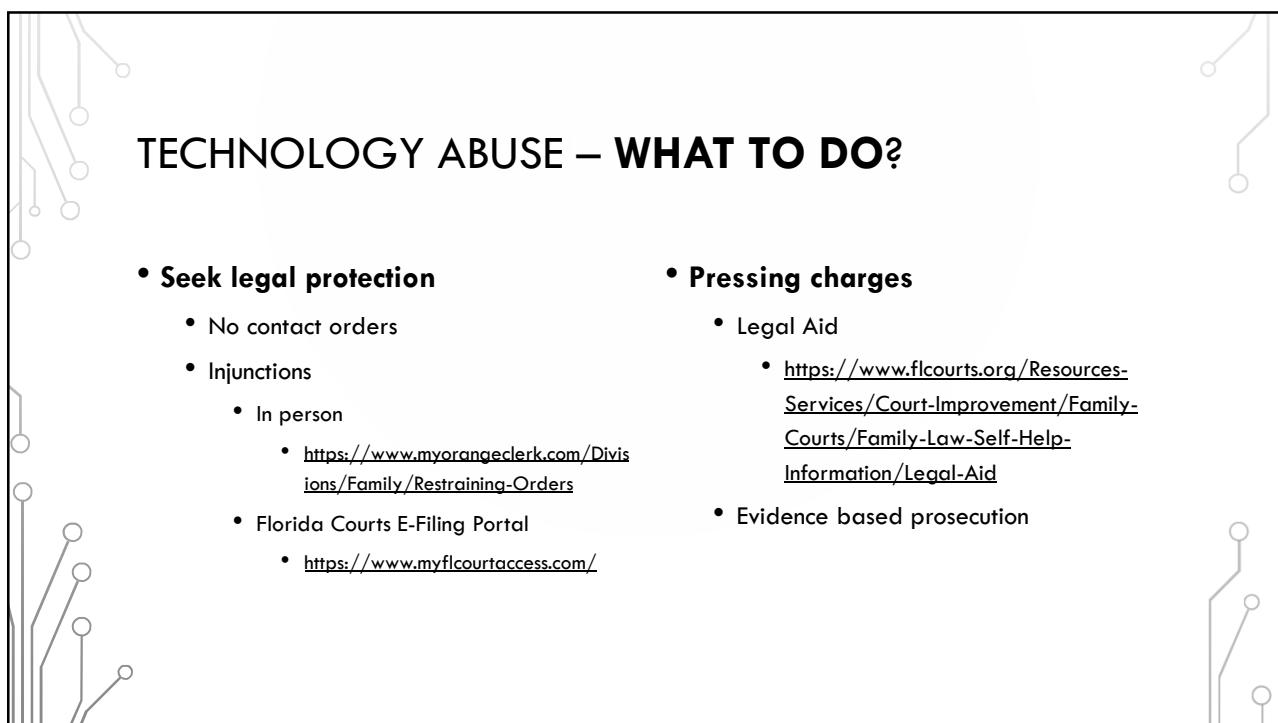
- Local law enforcement
- Florida Computer Crime Center
 - <https://www.fdle.state.fl.us/FCCC>
- FBI Internet Crime Complaint Center
 - <https://www.ic3.gov/>
- Website/platform flags

38

19



39



40

TECHNOLOGY ABUSE – WHAT TO DO?

- **Educate children, family, and friends**
 - I am Cyber Safe
 - <https://www.iamcybersafe.org/>
 - Family Online Safety Institute
 - <https://www.fosi.org/>
 - Online Safety for Kids & Families
 - <https://www.missingkids.org/NetSmartz>
- Facebook's Digital Literacy Library
 - <https://www.facebook.com/safety/educators>
- Safe Online Surfing (SOS) - FBI
 - <https://sos.fbi.gov/en/>
- STOP. THINK. CONNECT. Toolkit - CISA
 - <https://www.cisa.gov/stopthinkconnect-toolkit>

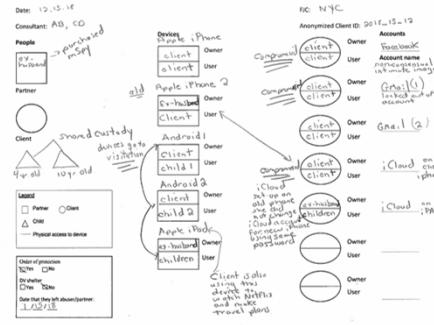
41

RESOURCES

42

COMPUTER SECURITY AND PRIVACY FOR SURVIVORS OF INTIMATE PARTNER VIOLENCE

- <https://www.ipvtechresearch.org/resources>
 - Technology Assessment Questionnaire (TAQ)
 - Privacy Checkup Guides
 - IPV Spyware Discovery Tool (ISDI)
 - Technograph
 - App Classification Guide



43

NATIONAL NETWORK TO END DOMESTIC VIOLENCE

- <https://www.techsafety.org/>
 - Survivor Toolkit
 - App Safety Center
 - Agency Use toolkit
 - Digital Services Toolkit
 - Confidentiality Toolkit
 - Legal Systems Toolkit
 - Judicial Toolkit



44

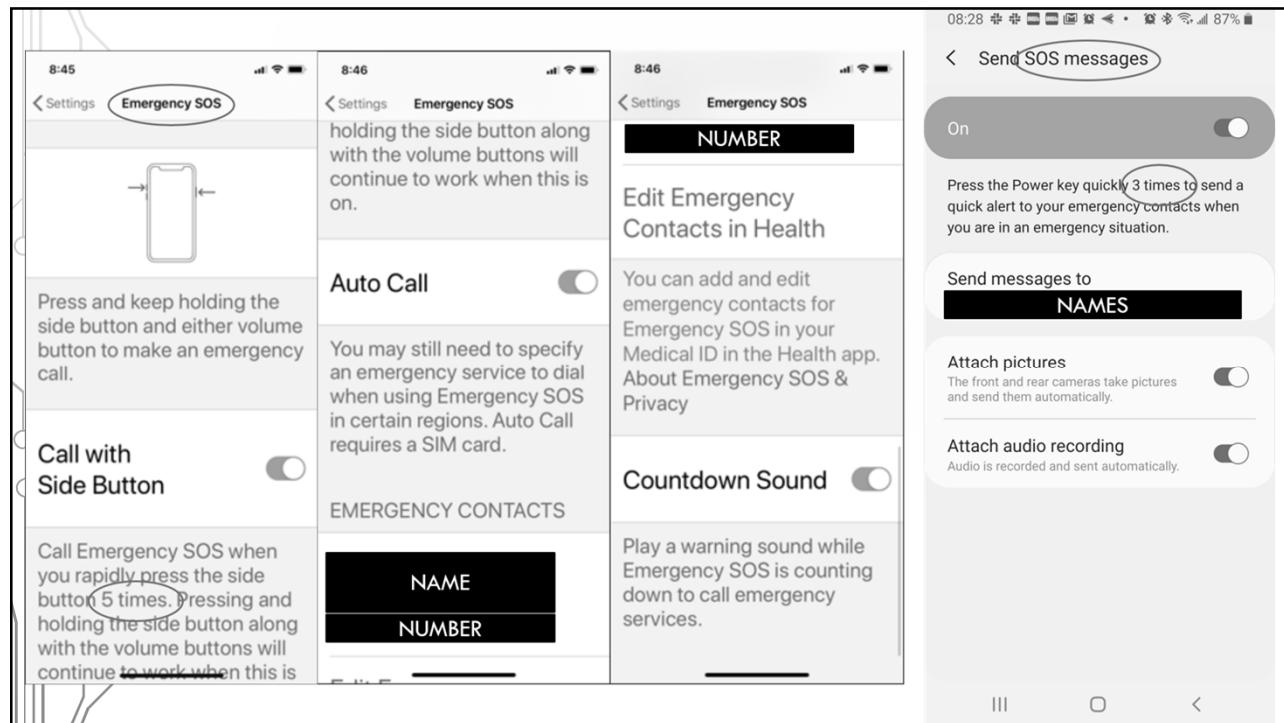
PHONE APPS AND FEATURES

- <https://techsafetyapp.org/>
- <https://www.circleof6app.com/>
- <https://kineticglobal.com/>
- <https://getbsafe.com/>
- <https://www.myplanapp.org/>

- SOS feature
 - Android
 - iOS
- Any phone will call 911 regardless of service subscription status



45



46

OTHER RESOURCES

- How to Gather Technology Abuse Evidence for Court
 - <https://www.flcourts.org/content/download/425826/4589773/how-to-gather-technology-abuse-evidence-for-court.pdf>
- DIY Cybersecurity for Domestic Violence
 - <https://hackblossom.org/domestic-violence/>
- Stalking online training from the National Center for Victims of Crime
 - <http://www.tech2stalk.com/>
- Tech and safety online course from the Florida Coalition Against Domestic Violence
 - <https://domesticviolencetraining.fcadv.org/>

47

OTHER RESOURCES

- Cyber Civil Rights Initiative (End Revenge Porn)
 - <https://www.cybercivilrights.org/>
- Gender and IoT (G-IoT) Resource List
 - <https://www.ucl.ac.uk/steapp/sites/steapp/files/g-iot-resource-list.pdf>
- Electronic Privacy Information Center
 - <https://epic.org/>
- Facebook's Safety Center
 - <https://www.facebook.com/safety/resources>
- Connect Safely
 - <https://www.connectsafely.org/>
- Media Smart
 - <https://mediasmarts.ca/>

48

24

OTHER RESOURCES

- Digital abuse article series
 - [https://www.thehotline.org/category/b
ehind-the-screens/](https://www.thehotline.org/category/b ehind-the-screens/)
- Social Media Security & Privacy Checklists – New York Times
 - [https://docs.google.com/document/d/
1ud1lLFkIG0BeLX9jIzJMxCPrm8-
cSeqPjU60nkhUPYA8/edit](https://docs.google.com/document/d/1ud1lLFkIG0BeLX9jIzJMxCPrm8-cSeqPjU60nkhUPYA8/edit)



49

THANK YOU!



50