TECHNOLOGY ENABLED DOMESTIC VIOLENCE

LATEST TRENDS & IMPACT
Gender-based violence is innovating.

We need to follow suit.
DEEPFAKES

FACE SWAPPING
The technique begins by analyzing photos or video of someone’s face, training an artificial intelligence algorithm to manipulate that face, and then using that algorithm to map the face onto another person in a video.
1. Victims are isolated with abusive partners.

2. Ushered victims, and those seeking to harm them, online.
   - Work, School, Socializing, Dating, etc.
In Today's World, Technology is Required to Survive & Thrive.
WHAT IS
TECH-ENABLED ABUSE?
1. Not New Abuse
   - Same abuse, different wrapper.
   - On a digital landscape.

2. Easier to Commit
   - Removes Barriers
   - Convenient
   - Accessible
   - Anonymous
   - Invisible

3. Greater Harm
   - Repeatable
   - Far-Reaching
   - Public
   - Permanent
   - Perpetual
Tech-enabled DV is on the rise and is here to stay.

Domestic Violence
97% of DV orgs report perpetrators use tech to abuse
101% increase in digital abuse calls to Nat’l DV hotline

Technology
81% of U.S. adults are online daily
94% of adults ages 18-49 own a smartphone
THE CURRENT PANDEMIC LANDSCAPE:

2 EMERGING TRENDS
Device & Account Sharing
"Full access to a person's phone is the next best thing to full access to a person's mind"

-Eva Galperin
#2
Emboldened Attackers

Normalization + Lack of Accountability
HOW TO ANTICIPATE & PREDICT TECH-ENABLED ABUSE
HOW CAN THIS....

APP, DATING SITE, SMARTPHONE, DEVICE, LOCATION TRACKER, SMART HOME, UPDATE, NEW TECHNOLOGY, ETC.
BE MISUSED TO....

Monitor, control, harass, (s)extort, threaten, humiliate, intimidate, impersonate, spread rumors, locate or otherwise abuse

....victims?
COMMON FORMS OF UNHEALTHY & ABUSIVE TECH-ENABLED BEHAVIOR
ACCESSING ACCOUNTS & DEVICES WITHOUT CONSENT
UNWANTED
CONTACT
SPY CAMERAS & LISTENING DEVICES

1. Unlikely
2. Look for other causes
3. Likely using
   a. WiFi
   b. Power
Download the Fing App network toolkit.

Use the free Fing App to identify connected devices, troubleshoot network and device issues, detect network intruders and run Wi-Fi and internet speed tests anywhere.
3 Reasons certain victims are at **EXTREME** risk of being harmed via technology.
1. Personal Connection.
2. No Hacking Skills Required, Just Opportunity.
3. Has or had the victim's trust.

(Access to passwords, devices, personal info, etc.)
FOR PROFESSIONALS WORKING WITH VICTIMS OF DOMESTIC VIOLENCE, THIS IS GOOD NEWS.
"Professionals don’t have to be experts to act when a victim is being harmed online or via technology. "
UPDATING PASSWORDS
COMPROMISED PASSWORD EXAMPLE
EXERCISE:

HAVEIBEENPWNED.COM
2-FACTOR AUTHENTICATION
DEFINITION:
AN EXTRA SECURITY FEATURE FOR ONLINE ACCOUNTS.

IF ENABLED, YOU’LL BE ASKED TO ENTER YOUR PASSWORD (STEP 1) AND A SECONDARY METHOD OF AUTHENTICATION, USUALLY A ONE-TIME CODE (STEP 2) SENT VIA TEXT MESSAGE TO YOUR PHONE.
TRUSTED & SAFE DEVICES
Huge security loophole that harms victims
○ Victim used attacker’s device
○ Auto-fill passwords
Meant to be convenient & save time
Feature offered by most major platforms
VERIFY
CONTACT INFORMATION
CONTACT
ADAM@ENDTAB.ORG

@ADAMRDOUDGE
1. Is there any effort underway to infuse computer science/tech classes and degrees with ethics/empathy/some form of moral compass?

• One hopes this will become a requisite course for all computer science/engineering students. Some schools may be raising these issues in their courses, but to my knowledge it’s not a uniform requirement. Inspiration for a course topic could come from a recent initiative by IBM, covering 5 design principles to combat DV, which can be found here.

2. When you get to discussing types of tech stalking, please share tech aided stalking and harassment using smart cars, like Tesla and other vehicles with GPS and remote access capabilities.

• Definitely agree. Location tracking via vehicles is a topic I include in my broader trainings. Like most smart devices, a car’s operating system can be misused to locate a victim or send an alert when the car passes a geographic boundary (geofencing).
3. Are the schools and universities doing anything to prepare for this? For example universities setting up policies to hold youth accountable who victimized Dept students.

- Some are beginning to adapt their policies and procedures to online and tech-enabled abuse, but this needs to occur nationwide. A current challenge is with the changes to Title IX regulations that have called into question whether online abuse qualifies as occurring “on campus”, which could make victims ineligible for title IX protections.

4. Are high schools preparing or at least aware of this? As a parent, how can I protect or prepare my child for this?

- I’m guessing this is about the deepfakes portion of the presentation. My honest answer is that nearly all highsads are unaware of this new threat and are not preparing for it. The best thing we can do is make children aware of this threat and suggest they make their social media profiles private (this is where photos for deepfakes can be collected). However, if an ex-partner or friend decides to create a fake, there’s little we can do to prevent it. Especially with new apps requiring limited photos to make the fake. Alerting schools to this threat is critical, so they can take steps to hold students accountable and have protocols in place when this does start happening in earnest on campuses.
Q&A

5. Do you have a list of Tech Experts that can testify competently in CA Courts regarding audio/video that has been altered?

• This goes to the detection issue. At present, a detection method doesn’t exist that can identify a fake with 100% accuracy. Those companies that are working on this issue include sensity.ai, fakenetai.com, reality defender 2020, etc.

6. Adam is there more men than women using this against their partners, THANK YOU!!

• While there are not statistics on this issue, the anecdotal evidence would confirm this to be true.

7. Would using a virtual background and a VPN help make virtual dating safer?

• Great question! Yes to the virtual background, this is definitely a tech-savvy safety planning measure we recommend to prevent dating abuse. Also, if the victim is going to share nudes, we recommend they do not show their face or identifying marks/tattoos in the photos to mitigate the impact of image-based abuse.

• A VPN is a great safety practice in general (especially if using public wifi), but I don’t know that someone could discern the IP address of a victim simply by video chatting with them. For example, we posed this concern to a group of experts about this risk on Zoom and they concluded that the IP address was not at risk of being disclosed. That being said, different video conferencing platforms may have different security flaws. At the end of the day, it wouldn’t hurt to use a VPN when video dating but I don’t know that it’s necessary.
8. Vehicles can now be tracked, accessed and even dangerously controlled through remote in real time by abusers. Can Adam please talk about how to stop or even prove this is occurring if manufacturers do not seem to be taking responsibility for victim safety. The technology is not meant to be used in this manner, but it is being used in this way to harm and harass abuse victims.

- Technology being misused to cause harm is the crux of most tech-enabled abuse and vehicles are no different. It comes down to including the online account/app associated with the vehicle in digital safety planning - updating the password, confirming the contact information, removing trusted devices, etc. Getting car manufacturers to contemplate the unintended uses of their tech is part of a broader challenge with tech companies in general.

9. Would you suggest using Vanilla Visa cards for Uber/Lyft/Instacart to protect ID? do you have other recommendations to help protect survivors/take countermeasures?

- I think the challenge here is that the victim would still be using a compromised rideshare or food delivery app, making the introduction of a vanilla visa card ineffective at addressing the security concerns. The key is to update those apps/accounts (or delete them and open new ones) to ensure the other party does not have access. Also, update settings to stop receipts going to the victim’s email in case the email is compromised.
10. Hi, what if you have housemates? Would Fing still help?

- Yes, I think it’s still effective. You could still inventory each device by asking housemates to confirm their devices, anything left over could be a concern. Also, if a camera or listening device does show up, it would raise red flags and possibly implicate a housemate.

11. How do you help someone find out if there is a GPS device hidden in their car?

- A good place to start is checking the data port under the dashboard. This is where mechanics plug in to run a diagnostic on the car’s computer system, but there are devices that can be plugged in here which can be misused to track the car, bluetooth calls, mileage, etc. Otherwise, it’s a matter of a thorough visual inspection (under car, wheel wells, trunk, under the dash, etc.)