

Sexual Violence in Digital Spaces

By Hieu Pham

Why This Training Matters

Technology is woven into the fabric of daily life — and into the dynamics of sexual violence.

1 in 5

College women experience
sexual assault

90%+

Of campus assaults involve
someone the victim knows

97%

Of 18–29 year olds
own a smartphone

Harm doers misuse technology to plan, commit, and cover up sexual violence. At the same time, digital trails can become critical evidence, and technology can empower survivors. Campus advocates and administrators must understand both dimensions to respond effectively.

Learning Objectives

1

Recognize

how technology is used to facilitate sexual violence on campus

2

Identify

specific apps, platforms, and features commonly misused by perpetrators

3

Apply

trauma-informed assessment questions when working with survivors

4

Develop

safety plans that address digital threats and privacy concerns

5

Understand

evidence preservation and legal considerations for tech-facilitated abuse

6

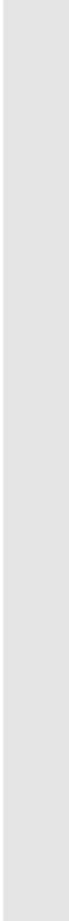
Connect

survivors with appropriate technology-specific resources



Understanding Tech-Facilitated Sexual Violence

How technology intersects with sexual violence — and why it matters for campus response



How Technology Intersects with Sexual Violence

BEFORE

- Targeting victims via social media
- Grooming through messaging apps
- Using dating apps to identify targets
- Researching victims' routines and locations
- Building trust through online communities

DURING

- Recording assaults on phones or cameras
- Live-streaming sexual violence
- Using location tracking to find victims
- Controlling victims via device monitoring
- Drugging facilitated through app meetups

AFTER

- Threatening to share intimate images
- Harassing survivors on social media
- Using tech to cover up evidence
- Impersonating survivors online
- Recruiting others to harass survivors

The Campus Context

Shared Digital Networks

Students are deeply interconnected through social media, class groups, and campus apps. Perpetrators may share mutual connections with victims, making online harassment more pervasive.

Power Imbalances

Community leaders like professors, coaches, RAs, and club leaders can misuse authority and access to databases, grading systems, and institutional tech to facilitate abuse.

Digital-First Social Life

College students conduct most of their social interactions through apps and platforms. Abuse that happens in these spaces feels inescapable when the digital environment is also their primary social world.

Peer Dynamics

Most campus sexual violence involves someone the victim knows — a classmate, friend, or partner. This means shared access to devices, accounts, passwords, and digital spaces.

Tactics by Relationship Type

Community Leaders

Teachers, coaches, RAs

Misusing messages to groom; accessing databases; threatening to share images; changing grades

Peers & Classmates

Friends, acquaintances

Creating synthetic intimate images (deepfakes); blackmailing into sexual activity; online harassment campaigns

Intimate Partners

Current or former

Monitoring devices and accounts; location tracking; threatening to share intimate images; controlling access to tech

Authority Figures

Employers, law enforcement

Misusing surveillance cameras; database access; seizing devices; limiting access to help resources

Key Principle

"Technology is not the enemy. The misuse is the problem. Tech can empower survivors as well as be misused to harm them."

Survivors have a right to technology. Advocates should never victim-blame around tech use.

Tech Can Be Misused To Harm

- Plan, commit, and cover up violence
- Harass and intimidate survivors
- Compromise privacy and safety

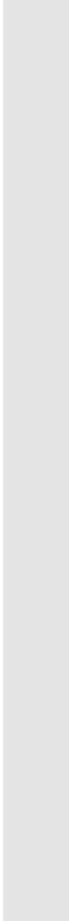
Tech Can Empower Survivors

- Document evidence via digital trails
- Increase privacy and personal safety
- Connect with support resources and community



Apps, Platforms & Technologies

Understanding the tools that are commonly misused in campus sexual violence



Social Media Platforms

Platforms students use daily that are commonly exploited

Snapchat

- Disappearing messages create false sense of safety
- Snap Map reveals real-time location to contacts
- Screenshots can be taken despite "disappearing" feature
- Used for sharing non-consensual intimate images

Instagram / TikTok

- DMs used for harassment and unwanted sexual content
- Fake accounts created to stalk or impersonate
- Location tags reveal daily patterns and routines
- Comments and posts used for public shaming

Facebook

- Groups and events reveal social connections
- Messenger used for grooming and coercion
- Old photos and posts mined for personal info
- Tagging and check-ins track movements

Messaging & Communication Apps

Telegram

End-to-end encryption, self-destructing messages, anonymous channels. Often used to distribute non-consensual intimate images in group channels that are difficult for law enforcement to monitor.

WhatsApp

Encrypted messaging with large group capability. Forwarded messages can spread intimate images rapidly. Location sharing feature can be exploited for tracking.

Discord

Voice and text channels popular with students for gaming and campus groups. Private servers can host harassment campaigns. Screen sharing can be exploited during video calls.

iMessage / SMS

Default texting on phones. Sexting coercion, threatening messages, and sharing intimate images. Messages may be backed up to shared cloud accounts without the victim's knowledge.

Dating & Hookup Apps

Dating apps are common among college students and present unique safety concerns

Tinder / Bumble / Hinge

Proximity-based matching can reveal general location; profiles share personal information; meetups with strangers carry safety risks

Grindr

Location precision is high; used by LGBTQ+ students who may not be out publicly; outing threats add layer of coercion

YikYak / Anonymous Apps

Anonymous posting on campus enables sexual harassment without accountability; rumors and threats spread rapidly

KEY RISKS TO ASSESS

- Did the perpetrator and survivor meet through an app?
- Does the perpetrator know the survivor's location through the app?
- Were explicit messages or images exchanged?
- Is the perpetrator using the app to contact or stalk the survivor?
- Are there other potential victims on the platform?

Location Tracking & Surveillance

Tracking Technologies

AirTags & Tile Trackers

Small devices hidden in bags, cars, or personal items to track a person's location without their knowledge

Find My / Family Sharing

Shared Apple/Google accounts allow real-time location monitoring; may have been set up during a relationship

Spyware & Stalkerware

Apps installed on victim's phone that monitor messages, calls, browsing, and location — often without any visible icon

Vehicle GPS

Hidden GPS devices in cars or accessing built-in vehicle tracking systems

Campus Surveillance Concerns

- Security cameras in dorms and buildings misused by those with access
- Smart locks and keycard systems log entry/exit patterns
- Shared campus Wi-Fi can reveal device locations
- Smart home devices (Alexa, Ring) in off-campus housing can be exploited
- Webcams on laptops and phones accessed via malware or remote access tools

AI-Generated Content & Deepfakes

Synthetic intimate images are an emerging and rapidly growing form of tech-facilitated sexual violence

What Are Deepfakes?

AI tools can now create realistic synthetic (fake) intimate images of a person using only their publicly available photos. These images are nearly indistinguishable from real photos. On college campuses, this is especially common among peers.

Campus Impact

- Used for blackmail, harassment, and humiliation
- Distributed through group chats and social media
- Victims may not know images exist until widely shared
- Causes severe psychological harm even though images are fake
- Difficult to fully remove once distributed online

TOOLS & RESOURCES

- [StopNCII.org](https://stopncii.org) — Tool to prevent spread of non-consensual intimate images (adults)
- [TakeItDown.NCMEC.org](https://takeitdown.ncmec.org) — For victims under 18
- Cyber Civil Rights Initiative — Legal assistance and advocacy
- 48+ states now have laws against non-consensual intimate images
- Federal TAKE IT DOWN Act (2025) — Criminalizes sharing NCII including AI-generated

Gaming, VR & Emerging Technologies

Online Gaming

Voice chat in multiplayer games is a common vector for sexual harassment. In-game messaging allows grooming. Gifting in-game items can be a manipulation tactic.

- Twitch, Discord, Xbox Live, PlayStation Network
- In-game voice and text chat
- Streaming platforms where harassment occurs live

Virtual Reality

VR environments enable virtual sexual assault through avatar groping and boundary violations. The immersive nature makes these experiences deeply traumatic.

- Meta Quest, VRChat, Rec Room
- Haptic feedback adds physical dimension
- Anonymity enables predatory behavior

IoT & Smart Devices

Connected devices in shared living spaces can be exploited. Smart speakers may record conversations. Smart home controls can be used for coercion.

- Smart locks, thermostats, lights
- Shared streaming and smart speaker accounts
- Baby monitors and home security cameras

Gaming, VR & Emerging Technologies

Online Gaming

Voice chat in multiplayer games is a common vector for sexual harassment. In-game messaging allows grooming. Gifting in-game items can be a manipulation tactic.

- Twitch, Discord, Xbox Live, PlayStation Network
- In-game voice and text chat
- Streaming platforms where harassment occurs live

Virtual Reality

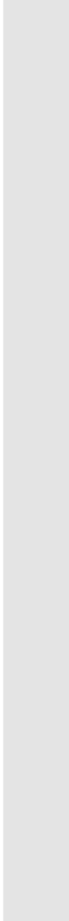
VR environments enable virtual sexual assault through avatar groping and boundary violations. The immersive nature makes these experiences deeply traumatic.

- Meta Quest, VRChat, Rec Room
- Haptic feedback adds physical dimension
- Anonymity enables predatory behavior

IoT & Smart Devices

Connected devices in shared living spaces can be exploited. Smart speakers may record conversations. Smart home controls can be used for coercion.

- Smart locks, thermostats, lights
- Shared streaming and smart speaker accounts
- Baby monitors and home security cameras



Assisting Student Survivors

Trauma-informed approaches to assessing and responding to
tech-facilitated sexual violence

Assessing for Technology Misuse

Use these questions as starting points — not as an intake form. Adapt as relevant over time.

PHYSICAL SAFETY & MONITORING

- Are you concerned about being harmed in person?
- Do you think this person might be tracking your location?
- Are your conversations being monitored?
- Does this person have access to your devices or accounts?

DIGITAL PRIVACY & REPUTATION

- Are you concerned about images or info being spread online?
- Is the offender impersonating you online?
- Are you concerned about information available about you on the Internet?
- Do you have concerns about your privacy or safety related to technology?

Types of Technology to Assess

When working with a survivor, consider all the ways technology could be involved

Social Media

Posts, comments, photos, video, live features, location

Messaging Apps

Texts, encrypted chats, group messages, voice/video

Dating / Hookup Apps

Profiles, messages, location-based matching

Tracking Devices

AirTags, GPS, location sharing features on phones

Gaming & VR

In-game chat, voice comms, streaming platforms

Smart Devices / IoT

Smart locks, cameras, speakers, doorbells, cars

Shared Accounts

Cloud storage, streaming, family plans, shared logins

Campus Systems

School email, LMS, databases, keycard access, Wi-Fi logs

Safety Planning with Technology

Safety planning must include digital safety — not just physical safety

Account Security

Help survivors change passwords, enable two-factor authentication, and remove the offender's access to shared accounts. Review which apps and services are linked.

Device Safety

Check for stalkerware or tracking apps. Review location sharing settings. Consider whether devices themselves are compromised or monitored.

Privacy Settings

Audit social media privacy settings. Review what personal information is publicly visible. Consider Google alerts for their name.

Communication Safety

Identify safe ways to communicate. Consider whether current messaging apps are monitored. Set up alternative secure communication channels.

Documentation

Create a plan for safely documenting evidence. Use a device the offender does not have access to. Store documentation in a secure location.

Digital Evidence Preservation

Steps for Preserving Digital Evidence

1 Screenshot Everything

Capture messages, posts, profiles, and timestamps. Include full conversation threads and meta data where possible.

2 Save Original Files

Download original photos, videos, and messages rather than relying on screenshots alone. Original files contain metadata.

3 Document the Timeline

Note dates, times, platforms, and usernames for all incidents. Keep a written log alongside digital evidence.

4 Preserve Context

Capture the surrounding conversation, not just the threatening message. Show who sent it, when, and from what account.

5 Secure Storage

Store evidence on a device the offender cannot access. Use a trusted cloud account or give copies to a trusted advocate.

FOR CAMPUS POLICE

- Digital evidence is time-sensitive — some platforms auto-delete content
- Request platform data preservation through legal channels promptly
- Do not access the survivor's device without consent and proper procedures
- Chain of custody applies to digital evidence
- Consider consulting with digital forensics specialists
- Coordinate with Title IX office on evidence needs

Privacy Concerns for Survivors

Survivors of sexual violence face unique privacy vulnerabilities in the digital age

Common Privacy Fears

- Intimate images being shared or posted online
- Personal information being doxed (address, phone, schedule)
- Being outed — LGBTQ+ identity, immigration status, etc.
- Online harassment, comments on news stories
- The offender monitoring their digital activity
- Police records or court documents becoming public
- Retaliation from the offender or their social network

How Advocates Can Help

- Audit what personal info is publicly available online
- Help configure privacy settings on social media
- Discuss options for content removal (NCII, deepfakes)
- Plan for potential triggers in news or social media
- Set up Google Alerts for their name
- Connect with organizations like Cyber Civil Rights Initiative
- Discuss reporting options and what each means for privacy

Empowering Survivors Through Technology

Documentation & Evidence

Digital trails left by perpetrators can be powerful evidence. Help survivors safely document incidents using their own devices and secure accounts.

Increased Privacy & Safety

Technology can help survivors increase their safety — encrypted messaging, privacy tools, location hiding, and security apps.

Connection & Healing

Online support communities, telehealth counseling, and anonymous reporting tools give survivors pathways to healing and justice.

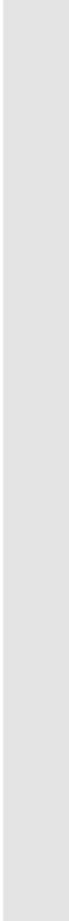
Reporting Tools

Apps like Callisto, campus anonymous reporting portals, and the Cyber Tipline offer ways to report that feel safe and controlled.



Legal & Institutional Response

Title IX, criminal law, and campus protocols for tech-facilitated sexual violence



Title IX & Technology-Facilitated Abuse

Title IX Coverage

Title IX prohibits sex-based discrimination in education, including sexual harassment and sexual violence. Technology-facilitated abuse that creates a hostile educational environment falls under Title IX — even when it occurs off-campus or online.

Forms of Tech Abuse Covered:

- Non-consensual sharing of intimate images
- Online stalking and cyberstalking
- Digital sexual harassment (unwanted sexting, etc.)
- AI-generated intimate images (deepfakes)
- Technology-facilitated dating/domestic violence
- Online retaliation against reporters

INSTITUTIONAL OBLIGATIONS

- Respond promptly to reports involving technology
- Investigate digital components with same rigor as in-person conduct
- Issue no-contact orders that include digital contact
- Provide interim measures (class changes, housing) when online harassment continues
- Train Title IX coordinators on tech-facilitated abuse
- Include technology misuse in student conduct policies
- Coordinate between Title IX, IT, and campus police

Reporting & Evidence for Campus Police

Receiving Reports

- Ask about technology involvement in every sexual violence report
- Document all platforms, apps, and devices involved
- Ask about shared accounts, location tracking, and monitoring
- Assess for ongoing digital threats and need for immediate safety measures
- Recognize that digital evidence may be on multiple platforms and devices
- Coordinate with the Title IX office early in the process

Digital Evidence Best Practices

- Act quickly — content on some platforms auto-deletes
- Request data preservation from platforms via legal process
- Maintain chain of custody for digital evidence
- Use forensic tools for device examination (with consent)
- Consider subpoenas for platform data (IP logs, messages)
- Work with digital forensics specialists when available

Important: Never access a survivor's devices without their informed consent. Explain what the examination involves, what data will be accessed, and who will see it. The survivor should feel in control of their own technology throughout the process.

Institutional Protocols & Collaboration

Effective response requires coordination across campus offices

Title IX Office

Investigate complaints; issue no-contact orders (including digital); provide interim measures; ensure policy covers tech abuse

Campus Police / Public Safety

Receive reports; preserve digital evidence; coordinate with local law enforcement; issue emergency protective orders

Counseling Center

Trauma-informed support; address impact of online harassment; safety planning; referrals to specialized services

IT Department

Assist with device security; help remove stalkerware; preserve digital records; advise on campus system privacy

Student Conduct

Adjudicate violations; enforce no-contact orders; address technology misuse in conduct code; impose sanctions

Dean of Students

Coordinate support services; implement housing/academic accommodations; connect offices; ensure survivor-centered response

Key Takeaways

1

Technology is not the enemy — misuse is the problem.

Survivors have a right to use technology. Never victim-blame around tech use.

2

Always assess for technology involvement.

Ask about devices, apps, accounts, and digital safety in every case of sexual violence.

3

Digital evidence is time-sensitive.

Act quickly to preserve evidence. Some platforms auto-delete content.

4

Safety planning must include digital safety.

Passwords, location tracking, spyware, and shared accounts all need to be addressed.

5

Collaboration is essential.

Title IX, campus police, counseling, IT, and student conduct must work together.

6

Stay current.

Technology evolves constantly. Regular training and updated policies are essential.

Resources

National Resources

National Sexual Assault Hotline: 800-656-4673

RAINN Online Chat: hotline.rainn.org/online

National Domestic Violence Hotline: 800-799-7233

Cyber Tipline (NCMEC): CyberTipline.org

StopNCII.org (non-consensual intimate images)

TakeItDown.NCMEC.org (for minors)

Tech-Specific Organizations

NNEDV Safety Net Project: TechSafety.org

Cyber Civil Rights Initiative: cybercivilrights.org

WomensLaw.org — legal info on tech abuse

OnlineSOS.org — online harassment resources

Victim Rights Law Center: victimrights.org

Without My Consent (merged with CCRI)

Thank you!

hieu@icadv.org