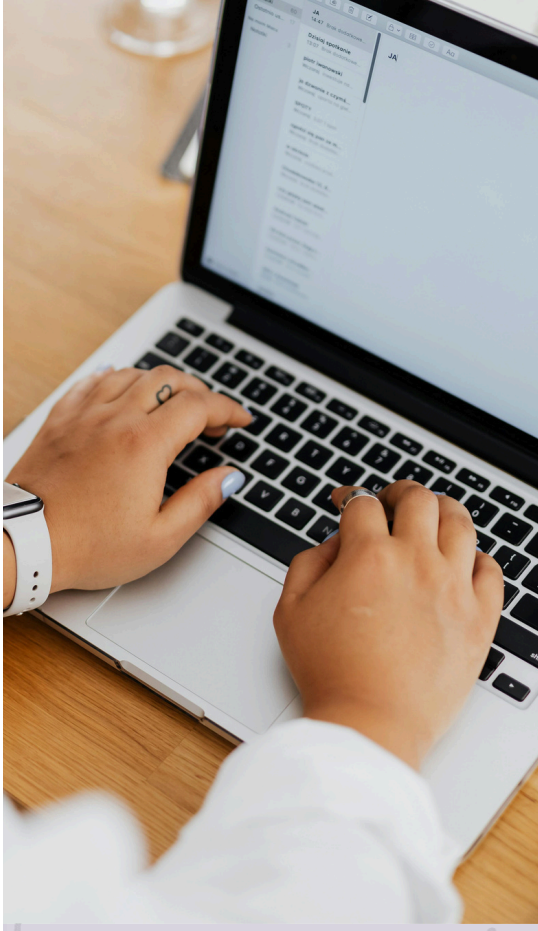
Technology-Facilitated Abuse and the Workplace



What is Technology-Facilitated Abuse?

Tech-facilitated abuse (TFA) is the use of technology to monitor, control, harass, stalk, impersonate, or harm another person. In workplace contexts, this can include unauthorized access to work accounts, tracking location through company vehicles or phones, or sending harassing messages through work email or collaboration tools.

How Is Workplace TFA Different from Other Forms of Abuse?

When abuse involves workplace technology, survivors face considerations that don't apply to personal devices, such as:

- Employer policies may restrict how accounts can be secured,
- IT departments need access to legitimately monitor workplace systems,
- Changing passwords or settings may require employer involvement,
- Survivors may be storing evidence of abuse on employer-owned devices, and
- Reporting abuse may affect a survivor's job security and relationships with colleagues.

One challenge survivors face is **knowledge asymmetry:** successfully communicating what is happening to IT, Human Resources (HR), or cybersecurity professionals may require industry-specific terms that survivors and their advocates do not know. This toolkit includes terms that can help bridge that gap and provide strategies to address TFA specific to the workplace.

FUTURES WITHOUT VIOLENCE®

WORKPLACES RESPOND TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER

About this toolkit

This toolkit was developed by Futures Without Violence. This project is supported by Grant No. 15JOVW-24-GK-06128-NRCW awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed on this toolkit or in any materials on this site, are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

For questions or technical assistance, fill out our Training & Technical Assistance form.

Examples of Workplace Technology-Facilitated Abuse (TFA)

Examples of Workplace TFA Against an Employee by a **Current or Former Intimate Partner**

Account compromise: Logging into your work email, Slack, or other accounts to read your messages or monitor your communications.

Constant contact with you or your co-workers: Flooding your work email, phone, or messaging apps with calls, texts, or messages.

Image-based abuse: Sending intimate images (real or AI-generated) to your boss, coworkers, customers, or organizational partners.

Location tracking: Monitoring your location through a company phone, vehicle GPS, or badge access records.

Impersonation: Accessing your work accounts to send messages as you or creating fake accounts in your name.

Schedule surveillance: Accessing your work calendar to know where you'll be and when.

Examples of Workplace TFA by a **Coworker or Supervisor**

Inappropriate surveillance through workplace software: Using shared drives, calendars, or project management tools to monitor your activities beyond work purposes

Misusing administrative access: A supervisor accessing your email, files, or communications without legitimate business need

Using monitoring tools for personal purposes: Accessing "bossware" data to track your location or activity for non-work reasons

Inappropriate contact: Sending harassing messages through work email, Slack, or other platforms

Weaponizing work systems: Manipulating schedules, assignments, or access privileges as a form of control

Employment Sabotage

Employment Sabotage includes behaviors intended to prevent a survivor from obtaining or maintaining employment. Research shows 83% of survivors report their partner has sabotaged their employment through tactics like constant calls/texts to work, spreading rumors to colleagues, destroying work equipment, or preventing them from getting to work.[1]

With technology being ever-evolving, abusive partners and people who cause harm have endless opportunities to use technology to sabotage their current or former partner's employment.[1]

The Scope of Employment Sabotage

- 74% of employed survivors report being harassed at work.[2]
- 83% of survivors report their partner has sabotaged their employment.[3]
- 60% of survivors have lost at least one job due to abuse. 90%[4] of employed domestic violence survivors report problems at work because of abuse.[5]

The following terms are forms of employment sabotage when the person causeing harm targets a survivor's workplace, colleagues, or professional reputation.

Doxxing

Disclosing online private information, such as non-consensual intimate images (NCII, frequently known as 'revenge porn'), home address or phone, sexual identity, HIV status, etc.[6]

Misusing Employee Monitoring Software or "Bossware"

Bossware is software that collects data about the employee by continuously monitoring them through their device and analyzing the data. It is most often used to confirm time, attendance and productivity. While this software may be installed for business purposes, this software can be misused by an abusive coworker or supervisor who has access to monitoring data. Examples include Hubstaff, Time Doctor, Teramind, and ActivTrak.

[1] https://iwpr.org/wp-content/uploads/2020/09/C475_IWPR-Report-Dreams-Deferred.pdf
[2] https://doi.org/10.1177/0886260506295380
[3] https://iwpr.org/wp-content/uploads/2020/09/C475_IWPR-Report-Dreams-Deferred.pdf
[4] Id.
[5] Id.
[6] https://www.techabuseclinics.org/ch-9-helping-with-tech-abuse

Employment Sabotage, cont.

Impersonation or "Catfishing"

Pretending to be the survivor to cause reputational damage or to facilitate proxy harassment (e.g., pretending to be the survivor on a dating website and tricking people into visiting the survivor's home).

Misusing Mobile Device Management (MDM)

Software and business practice that enables employers to track employee work devices, collect data on how the device is used, and manage those devices remotely.

Proxy Harassment or "Gang Stalking"

Arranging for members of a common social network or strangers to harass the survivor or signing the survivor up for unwanted messages.[1]

Sexually Explicit Digital Forgeries or "Deepfake"

Sexually Explicit Digital Forgeries refers to visual material that is digitally manipulated using machine learning algorithms to make it appear that a person is nude, partially nude, or engaged in sexual conduct. The image, however, is not "real."[2]

Swatting

Swatting refers to a harassment technique that entails generating an emergency law enforcement response against a target or victim under false pretenses. Harassers do this by making phone calls to emergency lines and falsely reporting a violent emergency situation. Harassers may disguise themselves through techniques like "ID spoofing" where they use software to appear like they are a local caller, when they could be calling from anywhere in the world.[3]

Tech-Facilitated Sexual Assault

Tech-enabled sexual assault is any sexually abusive or exploitative behavior carried out using technology tools or online platforms, including artificial intelligence (AI). It can include **image-based sexual assault**, which is sexually explicit visual content that is created or shared without the subject's consent. It can also include sextortion or using threats to distribute intimate content (either "real" or artificially created) to coerce the subject of the content into sharing more content, sending money, engaging in personal favors, or remaining in a harmful relationship.

[1] https://www.techabuseclinics.org/ch-9-helping-with-tech-abuse
[2] https://cybercivilrights.org/ccri-safety-center/#glossary
[3] Adapted from https://www.cloudflare.com/learning/security/glossary/what-is-swatting/

Safety Planning

A safety plan is a survivor-led tool that outlines a set of actions that can help lower their risk of experiencing violence. Safety plans are specific to an individual and consider their safety needs at home, in the community, and in the workplace.

Safety plans, best developed with a trained victim advocate, cover:

- **Safety in the home including options for alternative housing arrangements and items to have readily available in case of a need to quickly vacate the home;**
- **How to safely commute to school and/or work;**
- **Who can serve as an emergency contact; how to protect access to email, phone, and online accounts;**
- **Keeping children safe; and**
- **Strategies to promote emotional health.**

There are generally two types of safety plans in the context of the workplace:

- one specific to the person experiencing violence (personal safety plan) and
- one focused on the overall workplace (workplace safety plan).

Both are designed to reduce the chance that the perpetrator will be able to harass or abuse the individual at work.

Safety Note: *If you are concerned that someone is monitoring your computer or phone use, consider accessing this document from a safer device, such as a public library computer or a trusted friend's phone. Your internet and device use can be tracked. If you need immediate help, contact the National Domestic Violence Hotline: 1-800-799-7233 or text START to 88788.*

Resources for Survivors

If you or someone you know is experiencing tech-facilitated abuse or other forms of DVSAS, there are people who can help.

National Hotlines

- National Domestic Violence Hotline: 1-800-799-7233 | Text START to 88788 | thehotline.org
- National Sexual Assault Hotline (RAINN): 1-800-656-4673 | rainn.org
- StrongHearts Native Helpline: 1-844-762-8483 | strongheartshelpline.org
- VictimConnect Resource Center: 1-855-4-VICTIM (1-855-484-2846) | victimconnect.org

Technology Safety Resources

- Safety Net at NNEDV: Technology safety resources, documentation tips, and training | techsafety.org
- Clinic to End Tech Abuse (CETA): Research and resources on tech-facilitated abuse | ceta.tech.cornell.edu
- Coalition Against Stalkerware: stopstalkerware.org
- National Resource Center for Cybercrimes (NRCC): guidance for professionals | cybercrimesresource.org
- Tech Safety Canada: techsafetycanada.ca

Futures Without Violence

- Workplaces Respond National Resource Center: Futures Without Violence's employer resources | workplacesrespond.org
- Advancing Safety Through Employment Rights – Futures Without Violence's Survivor Employment Rights Initiative | workplacesrespond.org/employment-rights
- Legal Momentum State Law Guide: Employment rights for survivors by state | 50 State Survivor Guide

Acknowledgements:
Workplaces Respond extends its deepest gratitude to Lana Ramjit at the National Resource Center on Cybercrimes, Julia Holtemeyer at the Stalking Prevention Awareness Resource Center, and Chris MacDougall at Futures Without Violence for their consultation and support in the creation of this resource.

WORKPLACES RESPOND
TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER

Workplaces Respond provides technical assistance to workplace stakeholders seeking to better prevent and respond to domestic violence, sexual assault, stalking, and harassment impacting the workplace.

Scan this QR code to access the Resource Center.