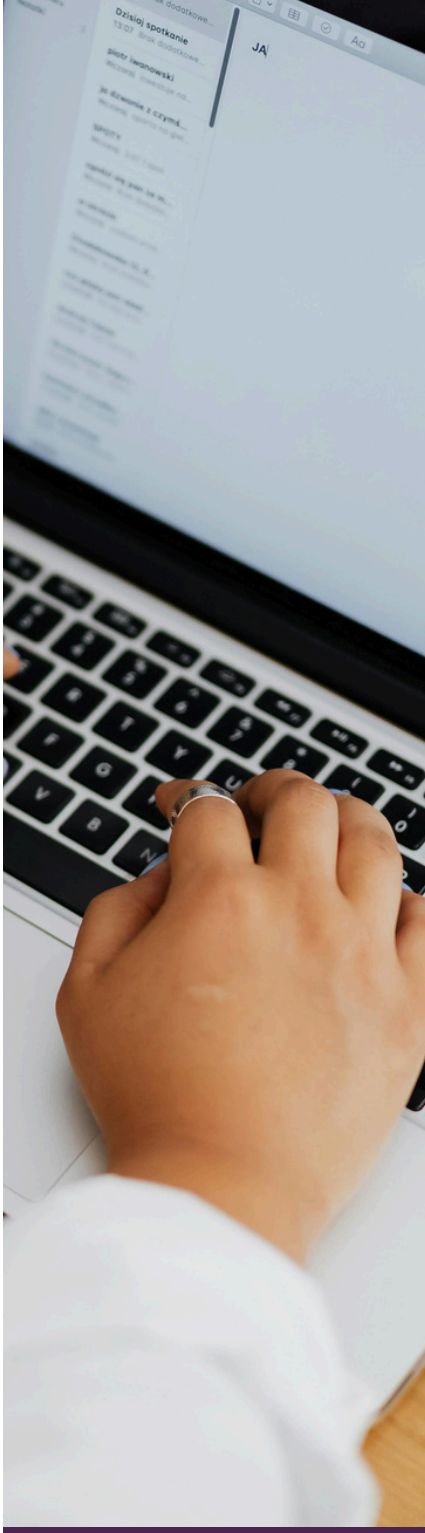
Workplace Technology-Facilitated Abuse

2026 Safety Planning Toolkit



Safety Note

If you are concerned someone is monitoring your computer or phone, consider accessing this document from a safer device, like a public library computer or a trusted friend's phone. 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.

FUTURES WITHOUT VIOLENCE®

WORKPLACES RESPOND TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER

TABLE OF CONTENTS

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 site 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.

Introduction

This toolkit addresses a specific gap in resources for survivors and advocates: tech-facilitated abuse (TFA) that occurs through employer-provided equipment and workplace software. While excellent resources exist for personal device safety, workplace technology presents unique challenges that require different safety planning strategies.

What is Tech-Facilitated Abuse?
Tech-facilitated abuse (TFA) is the use of technology to monitor, control, harass, stalk, impersonate, or harm another person.

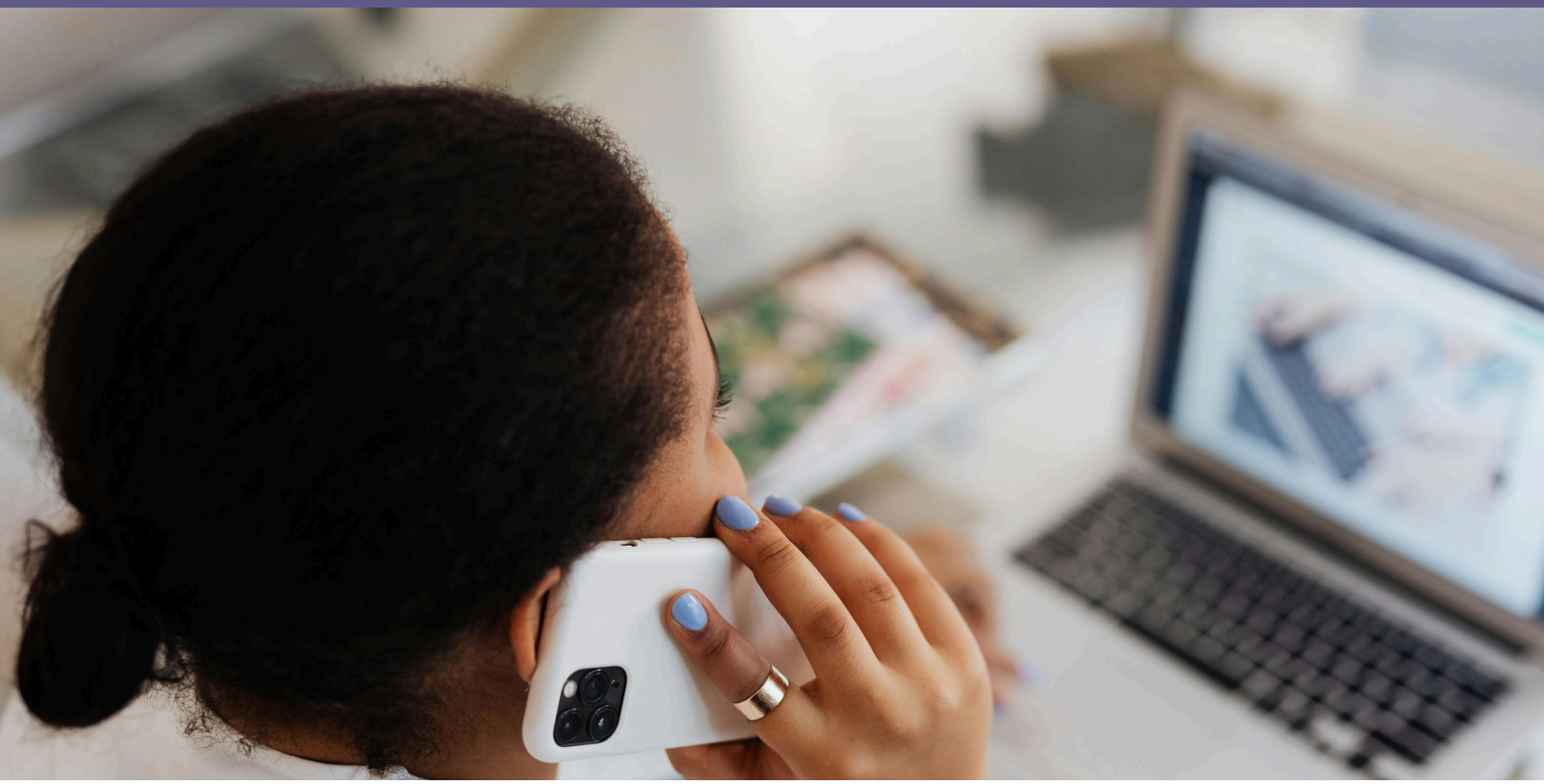
In the workplace, this can include unauthorized access to work accounts, tracking a person's location through company vehicles or phones, or sending harassing messages and images through work email or employer-provided collaboration software.

How Is Workplace TFA Different for Survivors?
When abuse involves workplace technology, survivors face considerations that don't apply to personal devices:

- 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.
- Reporting abuse may affect a survivor's job security and relationships with colleagues.

Knowledge Asymmetry
One of the biggest challenges survivors and advocates face is knowledge asymmetry:[1] successfully communicating what is happening to IT, Human Resources (HR), or cybersecurity professionals may require industry-specific terms that advocates and survivors do not know.

This toolkit bridges the knowledge asymmetry gap by defining common terms related to TFA and providing specific strategies to address workplace TFA.



HOW TO USE THIS TOOLKIT

For Workers Experiencing Violence

This toolkit provides information to help you understand your options. Every situation is different, and only you know what is safest for you. Consider connecting with a local victim service provider who can help you think through your specific circumstances. Advocates are trained to support individuals experiencing domestic violence, sexual exploitation, and stalking and can provide resources for support.

For Advocates

Use this toolkit alongside existing technology safety resources. The platform-specific guidance and assessment questions can help you support survivors navigating workplace-specific TFA.

---

(1) The phrase “knowledge asymmetry” was coined in Lana Ramjit, Nicola Dell, and Dana Cuomo. 2025. Trauma-Informed Organizational Coordination in Clinical Computer Security. Proc. ACM Hum.-Comput. Interact. 9, 7, Article CSCW502 (November 2025), https://doi.org/10.1145/3757683

Key Definitions

Artificial Intelligence (AI)
Artificial intelligence describes a computational system's ability to perform tasks that humans do. These tasks can include learning, reasoning, problem-solving, perception, and decision-making.[1]

Generative Artificial Intelligence describes a computational system's ability to create new data or objects based on what data it was trained on. [2]

"Bossware" or Employee Monitoring Software
Bossware is software that collects data about employees by continuously monitoring them through their employer-issued device and analyzing the data. It is most often used to confirm time, attendance and productivity. Examples include Hubstaff, Time Doctor, Teramind, and ActivTrak.

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.

Confidentiality
Confidentiality refers to the practice of safeguarding sensitive or private information and preventing its unauthorized disclosure, access, or sharing.

Logging or Audit Logging
Audit Logs are records that workplace systems automatically create showing who accessed what information and when. For example, Microsoft 365 and Google Workspace keep logs of who viewed shared documents, when emails were read, and login locations. These logs can be evidence of unauthorized access—or evidence that a survivor may need to access in order to document the TFA they are experiencing.

Key Definitions

Mobile Device Management (MDM)
Mobile Device Management is a 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.

Managed Security Service Provider (MSSP)
A Managed Security Service Provider is third-partner organization that provides network security services to a company, de-centralizing the control over employer-provided devices and software.

Safety Plan
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:

- the home, including options for alternative housing arrangements and items to have readily available in case the survivor needs to flee quickly;
- safely commuting to school and/or work;
- people who can be 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 chances that the perpetrator will be able to harass or abuse the survivor at work.

Key Definitions

Tech-Facilitated Sexual Assault
Tech-facilitated sexual assault is any sexually abusive or exploitative behavior carried out using technology tools or online platforms, including 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.

Privacy
Privacy refers to an individual's right to control their personal information, activities, and personal space. It encompasses the ability to determine what information about oneself is shared with others as well as the freedom to establish boundaries regarding one's personal life.

World of Work
A term from the International Labour Organization's Convention 190,[3] which recognizes that the "workplace" extends beyond a physical setting.

The world of work includes:

- physical workplaces,
- places where workers take breaks or meals,
- work-related travel,
- work-related communications (including digital),
- employer-provided housing, and
- commuting to/from work.

This broader definition of work is important because TFA can occur in any of these contexts.

Key Definitions

Employment Sabotage consists of 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.[4]

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.

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

Sexually Explicit Digital Forgeries or "Deepfakes"

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".[5]

Doxxing

Doxxing involves disclosing one's 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]

Key Definitions

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).

Proxy Harassment or "Gang Stalking"

Proxy harassment means arranging for members of a common social network or strangers to harass the survivor or signing the survivor up for unwanted messages.[7]

Swatting

Swatting is 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.[8]

Sources for Definition Section: (1) Russell, Stuart J.; Norvig, Peter (2021). A*rtificial Intelligence: A Modern Approach* (4th ed.). Hoboken: Pearson. ISBN 978-0-1346-1099-3. LCCN 20190474; (2) Zewe, Adam, *MIT News*, "Explained: Generative AI" (2023) (accessible at: https://news.mit.edu/2023/explained-generative-ai-1109; (3) C190 - Violence and Harassment Convention, 2019, International Labour Organization (2019); (4) Hess, Cynthia; Del Rosario, Alona (2018), *Dreams Deferred*, Institute for Women's Policy Research (accessible at: https://iwpr.org/wp-content/uploads/2020/09/C475_IWPR-Report-Dreams-Deferred.pdf; (5) Cyber Civil Rights Initiative, "CCRI Safety Center" (2026) (accessible at: https://cybercivilrights.org/ccri-safety-center/#glossary); (6) *The Technology Abuse Clinic Toolkit*, Clinic to End Tech Abuse (accessible at: https://www.techabuseclinics.org/ch-9-helping-with-tech-abuse); (7) *Id.;* (8) Cloudflare, "What is Swatting?" (2026) (accessible at: https://www.cloudflare.com/learning/security/glossary/what-is-swatting/).

When the Abuser is Not a Coworker

This section addresses situations where an intimate partner or harm doer who does *not* work at your organization is using technology to abuse, monitor, or harass you through your workplace systems.

Examples of Workplace TFA by a non-Coworker

- **Constant contact with you or your coworkers:** 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.
- **Impersonation**: Accessing your work accounts to send messages as you or creating fake accounts in your name.
- **Location tracking:** Monitoring your location through a company phone, vehicle GPS, or badge access records.
- **Schedule surveillance:** Accessing your work calendar to know where you'll be and when.
- **Account compromise:** Logging into your work email, Slack, or other accounts to read your messages or monitor your communications.

The Scope of Employment Sabotage

74% of employed survivors report being harassed at work.[1]

83% of survivors report their partner sabotages employment.[2]

60% of survivors have lost at least one job due to abuse.[3]

90% of employed domestic violence survivors report problems at work because of abuse.[4]

Cited Research: (1) Logan, T. K., Lisa Shannon, Jennifer Cole, and Jennifer Swanberg. 2007. "Partner Stalking and Implications for Women's Employment." Journal of Interpersonal Violence 22 (3): 268–91.; (2) Hess, C. and Del Rosario, A. (2018). Dreams Deferred: A Survey on the Impact of Intimate Partner Violence on Survivors' Education, Careers, and Economic Security. Retrieved from https://iwpr.org/wp-content/uploads/2020/09/C475_IWPR-Report-Dreams-Deferred.pdf. (3) *Id.* ; (4) *Id.*

Assessment Questions for Advocates

When working with a survivor who suspects workplace TFA, these questions can help clarify what is happening.

Questions:

1. What workplace devices do you use? (Computer, phone, tablet, vehicle)
2. Have you noticed any unfamiliar accounts or devices connected to your workplace devices?
3. What specific incidents made you suspect monitoring?
4. Does the person causing harm seem to know things about your work that they shouldn't? Can you give any examples?
5. Do you use the same passwords for work and personal accounts?
6. Does anyone else have access to your work passwords? Have you ever shared them?
7. Is your work calendar shared with anyone outside your organization?
8. Has the person causing harm ever set up or helped configure your work devices or accounts?
9. Does the person causing you harm know the name or email of your direct supervisor or their boss?
10. Do you have an employer-provided email address? Is it publicly available?
11. Does your employer-provided email address follow a standard format? (Example: Lastname-firstinitital@employerwebdomain.com)
12. Who at your organization helped you set up your workplace accounts?
13. Do you have a company vehicle? If so, does your company vehicle have GPS tracking? Who can access that data?

Adapted from the Clinic to End Tech Abuse's, *The Technology Abuse Clinic Toolkit*, "Technology Assessment Questionnaire" (accessible at: https://ca7f4499-b61e-4364-9012-d7ee2c81e754.filesusr.com/ugd/9e6719_321e70c917584da2a445ee1163af8c15.pdf).

Workplace Tech Abuse Documentation Log

Keep this documentation log in a safe place the abuser cannot access—consider using a personal email account, a trusted friend's device, or a paper copy kept outside your home.

Date &Time	
What Happened?	
Technology Involved	(Work email, Teams / Slack, company phone, AirTag, Vehicle GPS)
Evidence Saved?	(Screenshot, photo, forwarded email, etc. - described where saved)
Witnesses	
Reported to?	(Police Report #, HR contact, IT Ticket #)

Tip: Taking screenshots or photos with your personal phone can help preserve evidence even if your work device is later confiscated or wiped. Remember, your employer owns whatever is created on your employer-provided device, including evidence of harm.

Adapted from the National Network to End Domestic Violence's Documentation Tips for Survivors (Accessible here); Stalking Prevention Awareness Center's Stalking Incident and Behavior Log (accessible at: https://www.stalkingawareness.org/wp-content/uploads/2018/07/SPARC_StalkingLogInstructions_2018_FINAL.pdf).

Digital Safety Strategies by Platform

Important: Many of these digital settings may require assistance from your IT department to change in a corporate environment. Changing passwords may trigger alerts or affect other integrated systems.

Microsoft/ Microsoft 365/ Outlook

Signs of unauthorized access:

- Emails marked as read that you haven't opened
- Sent emails you didn't write
- Calendar invites you didn't create
- Inbox rules forwarding your email to unknown email addresses or ones you didn't allow

What you can check:

- Recent Sign-in Activity: Go to myaccount.microsoft.com > My Sign-ins
  - **Note**: Some organizations have additional security that shows your device as logged in from a specific location. Confirm with IT if you should expect to see your location or another location under "My Sign-ins."
- Inbox Rules: In Outlook, go to Settings > Mail > Rules. Look for unfamiliar forwarding rules.
- Calendar Access: Go to Calendar > select the three dots to the right of "Calendar" under "My calendars" > select "Sharing and permissions" to see who can view your calendar and what level of access they have.

What IT can check:

- Delegate Access: An administrator can go to Microsoft 365 Admin Center > Users > Active Users > Select your mailbox > Go to Mail tab and view under "Mailbox Permissions."

Digital Safety Strategies by Platform

Important: Many of these digital settings may require assistance from your IT department to change in a corporate environment. Changing passwords may trigger alerts or affect other integrated systems.

Google / Google Workspace

Signs of unauthorized access:

- Emails marked as read that you haven't opened
- Sent emails you didn't write
- Unfamiliar devices in your security settings
- Calendar invites you didn't create
- Inbox rules forwarding your email to unknown email addresses or ones you didn't allow
- Filters you didn't create
- Third-party app access you don't recognize
- Unfamiliar devices in your security settings

What you can check:

- Recent Activity: Scroll to bottom of Gmail inbox, click "Details" under "Last account activity."
- Filters: Settings > See all settings > Filters and Blocked Addresses.
- Forwarding: Settings > see all settings > Forwarding and POP/IMAP.
- Connected apps: Go to myaccount.google.com > Security > Third-party apps with account access.

Digital Safety Strategies by Platform

Important: Many of these digital settings may require assistance from your IT department to change in a corporate environment. Changing passwords may trigger alerts or affect other integrated systems.

Slack

Key Concerns:

- Slack shows your “presence” status (online/away) which can be used to track when you are working.
- Direct messages may feel private, but employers can access them.
- If logged in on multiple devices, messages sync across all of them.
- Custom status messages reveal your location or activities.

What you can check:

- Access logs sessions: Go to my.slack.com/account > Click “Access Logs” in the top right corner to view your logs > Click “Download access logs” to save a copy to your computer.
- Consider whether your status or profile information reveals your location or schedule.

Digital Safety Strategies by Platform

Important: Many of these digital settings may require assistance from your IT department to change in a corporate environment. Changing passwords may trigger alerts or affect other integrated systems.

Zoom

Key Concerns:

- Calendar integrations may reveal meeting schedules.
- Uninvited users can access meetings and share harmful images or information in real time.
- Meeting recordings may be accessible to others.
- If someone has your Zoom credentials, they can join the meeting as you.

What you can check:

- Uninvited User In a Meeting: Locate and click on the participants icon (typically at the bottom of the Zoom window) > select the “block” option from the dropdown menu > Confirm the block.

Note: Only hosts can block users or Zoom guests. Consider notifying IT and HR in writing if you think a person causing you harm may access your workplace Zoom. Provide their email address, user name, and/or phone number.

Using Workplace Equipment to Document Abuse

Survivors may use employer-issued devices to document abuse—for example, using a work phone to take photos of injuries. This can be critical evidence for a case against the person causing harm, but using workplace equipment to document abuse comes with risks.

The Risk: "Misuse of Workplace Equipment"

Most employers have policies restricting personal use of work devices. If a survivor uses a work phone to document abuse, this could violate those policies—even though the documentation is for safety purposes. Additionally, employers own whatever is created or captured using an employer-owned device. This means that images of abuse may technically belong to your employer if they are held on an employer-issued device.

Example - New York ITS Case (2019-2020)

An employee of New York State's Office of Information Technology Services (ITS) was experiencing domestic violence from her husband, who worked for a different state agency. He filed a complaint that she was "misusing" her state-issued phone. During ITS' investigation, the employee disclosed she was using her work phone to document his abuse—she could not use her personal one because he monitored it.

Despite disclosing domestic violence and her request for the recordings and photos on the phone that was evidence for her court case, ITS confiscated her phone and continued the disciplinary process. She was issued a warning for "misuse of workplace equipment" and denied access to her documentation.

Source: New York State Offices of the Inspector General, "Investigation of the New York State Office of Information Technology Services and Office of General Services Domestic Violence Incident Response," April 2022.

Template: Reporting Non-Coworker Workplace TFA to HR/IT

Important: This letter is an example of how a survivor can notify HR or IT of suspected tech-facilitated abuse (TFA). It is not legal advice. Consult an attorney licensed in your state or territory before adapting this letter to your situation or contacting your employer. Making this request does not guarantee a positive outcome.

To: [*HR Representative / IT / Security / Supervisor]*
From: *[Your Name]*
Date: [*Date*]
Re: *Security Concerns Regarding My Work Accounts*

To Whom It May Concern:

I am writing to report a security concern regarding my work accounts and devices. I have reason to believe that someone outside our organization may have unauthorized access to my [work email / calendar / phone / other systems].

I am requesting the following assistance:

1. A review of recent login activity and any unusual access to my accounts.
2. A password reset for my work accounts.
3. A review of any forwarding rules, delegates, or shared access on my accounts.
4. [If applicable: A review of who can access GPS/location data for my company vehicle/phone.]
5. Guidance on any additional security measures I should take.

This is a personal matter. Please keep this request confidential. I am happy to discuss further if helpful.

Thank you for your assistance.
[Your Name]

When the Abuser is a Coworker or Supervisor

When the person causing harm works at your organization, the dynamics are different. This person may have a *legitimate need to access* some workplace systems, making it harder to identify what constitutes misuse.

Power dynamics—especially if the person causing harm is a supervisor—also add complexity to reporting.

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.

Additional Assessment Questions

In addition to the **Assessment Questions for Advocates** on page 11**,** consider asking:

1. What is the person's role? Do they have supervisory authority over you?
2. Do they have a legitimate reason to access your work systems or data?
3. Have you noticed them accessing information they shouldn't need for their job or outside of their typical work hours?
4. Has the behavior been documented in any work communications?
5. Are there witnesses to any inappropriate technology use?
6. Is there anyone in HR or management you trust to report this to?

Template: Reporting Coworker or Supervisor TFA to HR

Important: When the person suspected of tech-facilitated abuse (TFA) is a coworker or supervisor, reporting has different considerations. An internal investigation will likely follow. Retaliation is possible. This template is not legal advice. Consult an employment attorney licensed in your state or territory before adapting this letter to your situation or contacting your employer. Making this request does not guarantee a positive outcome.

To: [*HR Representative / IT / Security / Supervisor (if not harm doer)]*
From: *[Your Name]*
Date: [*Date*]
Re: *Report of Inappropriate Use of Workplace Technology*

To Whom It May Concern:

I am writing to report concerns about inappropriate use of workplace technology by *[Name and Position, if comfortable sharing, or "another employee"]*. [*Describe specific incidents, including dates, times, and any witnesses. Focus on observable behavior rather than speculations about intent.]*

I am requesting:

- This matter be investigated;
- My accounts and access by reviewed for unauthorized access;
- Audit logs showing unauthorized access be provided to me;
- Appropriate measures be taken to protect my safety at work, including:
    - [If applicable: that I am not required to work directly with/report to this person during the investigation.]

I am concerned about retaliation and request this matter be handled confidentially to the fullest extent possible.
[*Your Name]*

Resources

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:

- 1-855-484-2846 | victimconnect.org

Legal Momentum Employment Rights of Survivors Hotline:

- 1-800-649-0297 | Help@LMHelpline.org | legalmomentum.org

Technology Safety Resources

SafetyNet at NNEDV: techsafety.org

Clinic to End Tech Abuse (CETA): ceta.tech.cornell.edu

Coalition Against Stalkerware: stopstalkerware.org

End Tech-Enabled Abuse (EndTAB): endtab.org

Cyber Civil Rights Initiative: cybercivilrights.org

Futures Without Violence's Workplaces Respond

Workplaces Respond to Domestic and Sexual Violence is a National Resource Center offering free resources, training, and technical assistance to employers, workers, and advocates to prevent and respond to domestic violence, sexual assault, stalking, and sexual harassment (DVSASSH) impacting the workplace. Learn more about our resource center.

FUTURES WITHOUT VIOLENCE®

WORKPLACES RESPOND TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER

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 (SPARC), Carrie Goldberg and Naomi Leeds at C.A.Golberg PLLC, Adam Dodge at EndTab, and Chris MacDougall at Futures Without Violence for their consultation and support in the creation of this resource.

SCAN THIS QR CODE TO ACCESS THE 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.

For questions or technical assistance, contact:
workplacesrespond@futureswithoutviolence.org

FUTURES WITHOUT VIOLENCE®

WORKPLACES RESPOND TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER