Disaster-Ready Cybersecurity Guidelines:

Building resilient support systems for domestic violence survivors

NRCC

CybercrimesResource.org

TechSafety.org

This resource was prepared by Naomi Meyer, Dea Angeles Quiroz, & Alex Worsham from the University of Washington in conjunction with the Safety Net Project at the National Network to End Domestic Violence (NNEDV) and the National Resource Center on Cybercrimes Against Individuals (NRCC).

August 2026.

This document is meant to be helpful for program managers, advocates, and IT providers. Since it is quite long, these guidelines are divided into several sections, listed in the Table of Contents. Some of the content is covered repeatedly or links to other sections of the document. This allows for easy selection of specific sections without having to read the entire document.

This project is supported by Grant No. 15JOVW-24-GK-02960-MUMU awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Department of Justice.

Table of Contents:

1. Cybersecurity during natural disasters

Each natural disaster is a reminder that victim service programs should be prepared, especially since they are becoming more common. This has led to domestic violence survivors and providers facing increased difficulties as they navigate crisis or emergency situations. During the course of a disaster, survivors often become more exposed and underprotected from different forms of abuse. They may face added physical harm, displacement, and limited access to safety resources because of these events. Natural disasters create complex challenges for local victim service providers, making access to or continuity of services difficult. This is often due to compromised infrastructure, damaged communication systems, or shelters being made inaccessible because of damaged roads and local infrastructure.

What are the cybersecurity threats faced by survivors during disasters?

The cybersecurity threats that DV survivors may already face can be exacerbated by disasters. This may result from weakened infrastructure and compromised access to secure communication. Risks include, but are not limited to:

- Technology-facilitated abuse such as location tracking, stalkerware, and using compromised (e.g. damaged, insecure, or abuser-controlled) devices.
- Damaged local infrastructure that limits access to secure communication methods and power sources
- Exposure of location to abusers due to limited options for shelter and the potential necessity of having to provide identifying information while seeking aid.
- Loss of access to digital files. For many survivors, digital files contain documentation of the abuse, or legal documents such as those needed to prove identity and residency.

Why do local victim service providers need to be prepared to support survivors and their families in disaster scenarios?

Natural disasters amplify vulnerabilities. They often disrupt traditional support systems and limit service provider capacity to communicate, provide resources, or safety plan. DV survivors and their families may become isolated and unable to access support such as legal protections. Service providers can mitigate this by planning in advance, in order to ensure service continuity as much as possible. Providers can engage in proactive training, set up resilient communication channels, and use agency tech best practices. In the event of a disaster, this can help increase the safety of survivors and their families.

2. Building resilient support systems for local victim service providers

How do we define a resilient cybersecurity support system?

A resilient cybersecurity support system is one able to provide support that helps survivors and their families that helps them maintain technological needs, even during extremely disruptive events like natural disasters. These could include digital safety, communication, and access to resources. Such a support system includes both human and technological components: trauma-informed staff, pre-established survivor centered communication methods, and emergency response protocols.

How can victim service programs keep services functioning during disasters?

It can be difficult to keep services functioning during natural or human-made disasters. For this reason, it is important to prepare ahead of time. One way programs can prepare is to build out and maintain a

Business Continuity Plan (BCP) and an Incident Response Plan (IRP). A BCP outlines how essential services continue during and after a disruption such as a natural disaster. It should address operational concerns like relocating staff, maintaining shelter services, accessing backup systems and communicating with both survivors and stakeholders. The next section of this document defines IRPs in more detail.

What external partners are available to collaborate with local victim service programs?

Programs may not have the capacity to build new relationships with stakeholder agencies in the midst of a disaster. It is better practice to build them *before* the disaster happens. Some examples of potential external partners include:

- Emergency management agencies (FEMA, State, local or county agencies).
- First responders.
- Public health authorities.
- Government agencies.
- Legal aid organizations.
- Private sector and community-based organizations.

Ideally, state/territory domestic violence coalitions would be involved in state/territory-level disaster response planning. In practice, this may or may not be the case, and may or may not be something that these coalitions have to do. Even so, programs can develop key partnerships as part of their external relations work. Developing key partnerships before they are needed will allow programs to coordinate a rapid and efficient response to emergencies in the face of a disaster.

How can staff best be trained to provide digital support services during disasters?

In addition to other ongoing training, organizations may provide disaster-related training at staff, in-service, or peer supervision meetings. These trainings should include the technical aspects of providing digital support, while interweaving emotional safety aspects throughout. This helps ensure that staff have a working understanding of digital privacy, secure communication methods, and how to recognize technology-facilitated abuse (TFA), with the added constraints of a natural disaster scenario. Training can be ongoing. It can take several different approaches, some of which include:

- Simulations based on likely scenarios to test the organization's preparedness.
- Discussion-based meetings where team members talk about their roles during a specific hypothetical emergency situation and go through their response, plan and capabilities ("table top exercises").
- Drills to practice specific emergency response tasks (which could include other types of emergencies as well as disasters) regularly.
- Role playing. This can help staff become confident while responding under pressure.

Staff can also be encouraged to learn more about tech safety by reading this website, requesting a training, or requesting technical assistance. Technical assistance may be ideal if the organization or a staff member needs help with a specific situation or question.

3. Incident response planning (IRP) for local victim service providers

What is an Incident Response Plan (IRP), and why is it important?

- An *Incident Response Plan (IRP),* is a structured, pre-established set of protocols that an organization prepares in order to respond and recover from emergencies, such as a natural disaster, that threaten its ability to keep providing services. An IRP can include roles, responsibilities, secure communication alternatives, coordination with third parties, or prioritization and protocols for reporting and assessing performance.
- The National Institute of Standards and Technology (NIST) outlines steps and best practices to establish, manage, and execute an effective IRP. Local victim service providers should consider modeling their IRPs after the NIST Incident Response Framework. This framework is divided into four phases: 1. Preparation, 2. Detection and Analysis, 3. Containment, Eradication and Recovery, and 4. Post-Incident Activity. Learn more at NIST Incident Response.

Why should local victim service providers build and maintain IRPs as preparation for natural disasters?

Organizations that support domestic violence survivors and their families should build and maintain IRPs to adequately prepare for natural disasters and other types of emergencies. This can help preserve continuity of survivor support services during disasters of all kinds. These kinds of emergency situations can lead to damaged infrastructure, power outages, and/or loss of access to physical facilities. An IRP provides a structured approach tailored to each organization by outlining contingency plans, roles, responsibilities, and predefined protocols.

How can an IRP be tailored to focus on support for survivors and their families?

Local victim service providers are especially well-positioned to adopt a trauma-informed and survivor-centered approach in developing their customized Incident Response Plans (IRP), as they are already educated in these principles. An IRP can be adapted to serve survivors and their families before, during, and after disasters by focusing on the Preparation and Containment parts of the NIST framework. This can help facilitate survivors' continuous access to resources throughout the duration of a disaster. Programs developing IRPs should consider communication resilience, cybersecurity, data protection, and physical and emotional safety - considerations that extend to staff and volunteers as well as survivors. Additional key aspects may include collaborations with external partners to receive or provide training, crisis management, and recovery.

One way in which an IRP for a victim service provider may be atypical, is the role of safety planning. Because situations of abuse and stalking are so individualized, often involving very different factors than those considered by mainstream security industries, a general "best practice" may not be the safest practice for a particular survivor. An IRP cannot possibly include every possible circumstance, but it can specify that providers should engage in technology (and other) safety planning during the Preparation phase (i.e. before a disaster actually happens).

In the following sections, there are several options listed as steps that survivors might take. These options should be discussed as part of safety planning, and not imposed on survivors as something they "have to" do.

What should an IRP include?

An effective IRP for victim service providers should be centered on support for survivors and their families directly, while considering traditional disaster management practices such as those used in other industries like healthcare and emergency management organizations. These plans should include psychological, legal, and digital safety needs for survivors and their families, taking into account that survivors vary in their experience with and access to technology. Some possible items to include are:

- Policies and procedures to switch, when possible, to encrypted messaging apps that can be used offline.
- Digital safety planning checklists for survivors and providers to discuss in advance of any disaster. The potential steps to consider while safety planning may include disabling geolocation, bluetooth, and/or Internet of Things ("IoT" or "smart") devices.
- Checklists of actions for providers to take to minimize data collection and location exposure.

What overall cybersecurity strategies are recommended?

We suggest that organizations use a *layered defense strategy* is the best practice. This means having multiple types of protection in place. When feasible, there are several different approaches that organizations may be able to use:

- Providing pre-scanned clean devices, such as safer phones.
- Considering secure communications apps such as Signal and Briar, while also respecting survivor constraints and needs. It is important to meet survivors where they are at technologically, while also offering them options they may not have known about. It can be helpful to have these discussions early in an advocate's relationship with a survivor.

- Training staff in privacy-preserving data practices, including minimizing data collection and having thoughtful retention and deletion policies.
- Keeping secure physical document backups.
- Properly storing sensitive information.

Learn more with these Safety Net resources:

- Encryption Basics for Programs Serving Survivors of Gender-Based Violence
- Selecting a Database
- Confidential Shelter Locations & The Internet: How Information Gets Online & What To Do About It

4. Communication strategies to increase digital safety during disasters

How can survivors best communicate with local victim service providers during a disaster?

As with all areas of survivor services, "best" depends on a survivor's individual needs. In areas where there may be high or impending disaster risk, survivors and advocates can discuss communication as part of regular safety planning. This provides advocates with an opportunity to bring up options that a survivor may not have been aware of. These include:

- Encrypted *offline* communication apps like Briar. These apps allow users to communicate without internet access (usually by using Bluetooth technology) over relatively short distances). This would allow survivors who can safely install an app on their device to communicate with their support system even in the case of internet outage.

- Peer-to-peer mesh network apps. These also allow communication without the internet. They leverage multiple devices as "nodes," which allows them to transmit messages over longer distances. Some examples are Meshtastic, GoTenna Mesh, and DittoChat.
- Other tools such as radios, solar-charged phones, or satellite phones. These require special hardware, and therefore are generally more expensive. However, if a survivor is able to keep this extra device safe until it is needed, it reduces the dangers for some survivors in installing an app on their regular devices.

Please note that Safety Net and NNEDV do not endorse these or any other products. We list them as examples to help providers find a starting point for researching this aspect of communications planning.

To the greatest degree possible, programs should offer the availability of multiple communication options for survivors, which allows survivors to determine which options are safest and most useful for them. This includes meeting survivors where they are at technologically. A survivor may not want to or be able to use unfamiliar apps or devices. The potential security benefits of such options may not outweigh other safety concerns, logistical difficulties, or other barriers. Safety Net's Digital Services Toolkit: Using Technology to Communicate with Survivors can assist programs in many areas of communications planning.

Is public Wi-Fi recommended for safe communication during disasters?

Public Wi-Fi networks are usually considered not secure by cybersecurity experts. These networks can expose anyone using them, even if used for a short time, to surveillance or data interception. However, during a natural disaster internet network options are likely to

be limited. A survivor may decide that the benefits of internet access outweigh the risks - especially if they do not believe that the abuser is technologically sophisticated enough to take advantage of Wi-Fi vulnerabilities - and use any Wi-Fi that might be available. In these cases, installing a Virtual Private Network (VPN) beforehand, and disabling file sharing, are potential ways for survivors who control their own device settings to reduce risk. You can learn more about Wi-Fi through Safety Net's **WiFi Safety & Privacy: Tips for Victim Service Agencies and Survivors** resource.

How can local victim service providers maintain confidentiality and protect the data of survivors and their families during disasters?

To the extent possible, organizations should maintain their normal data governance and confidentiality practices. Compromised infrastructure, and the disruption of digital systems and communication channels, can increase the risk of unintentional data exposure. As always, organizations should implement data minimization strategies and collect only essential data ("data minimization"). Outside of appropriate case management databases, it is better to use pseudonyms or alternative IDs to protect the identities of survivors and their families.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework and Zero Trust principles can be used to improve programs' overall cybersecurity, especially during emergency situations. A program's IT provider should be able to assist in understanding and implementing these.

It may be helpful, when a program first starts working with a survivor, to ask them what communication platforms they are comfortable with, and offer them information and options, including encrypted options like Signal or WhatsApp. It is important to center survivor autonomy and meet survivors where they are. It is also important to make sure

they have accurate information and know about options they may not have realized existed.

You can learn more about confidentiality and data security by reading the materials in the Confidentiality Toolkit and the Data Security Checklist to Increase Victim Safety & Privacy.

5. Disaster-ready personal device security guidelines

How can survivors and their families best protect personal devices during a disaster?

As part of the safety planning process, advocates should discuss emergency electronics needs with survivors. This might include information on maintaining fully charged devices whenever possible, and having emergency batteries or solar chargers available. To reduce the risk of location tracking, there are features that survivors should know how to turn off if it makes sense for their circumstances and when it is not essential to use them. These include:

- Location services,
- Bluetooth, and
- Wi-Fi (if a survivor has an unlimited data plan, they may be able to use this data plan for internet access instead of Wi-Fi).

Strong password or passkey protection is recommended. Depending on the survivor's circumstances, they may also want to use multi-factor authentication, biometric locks, and/or regular data backup. You can learn more by reading Safety Net's Passwords: Increasing Your Security resource.

Physical security of devices is also important. Survivors and their families may want to plan for secure locations in which they can keep their devices, or to keep the devices with themselves at all times. Waterproof bags can prevent devices being destroyed by rain or

flooding, and need not be expensive. A regular-sized Zip-Loc bag can fit a phone, a gallon-sized one can fit some tablets. As of this writing, there are waterproof laptop bag options that cost under $50, and even a few that cost under $30.

You can learn more digital safety for personal devices with Safety Net's **Technology Safety & Privacy: A Toolkit for Survivors**. The resources in this toolkit are meant for advocates to be able to discuss with survivors.

What additional resources are available for survivors and their families?

The National Network to End Domestic Violence (NNEDV) provides a variety of resources. These include Safety Net's **resources** for survivors and providers. In addition to Safety Net's technology safety assistance, NNEDV offers technical assistance to providers and state/territorial/tribal coalitions on **a range of topics**. Furthermore, NNEDV offers assistance to survivors through the **WomensLaw legal information email hotline** and credit-building **Independence Program** microloans.

Which apps provide encrypted communications?

Encryption helps protect information from unauthorized and unwanted access. Victim service programs should use encryption to protect data, communications, and websites whenever possible. Survivors can also use it to help protect their devices and communications. Options for encryption are available on most smart devices and online platforms. You can learn more about encryption (including its limitations) in our **Encryption Basics for Programs** resource.

There are several different apps that offer end-to-end encryption (security for data that is in transit between devices, such as a message, call, or email. Safety Net and NNEDV do not endorse products, but we

provide these examples, all of which offer end-to-end encryption as of September 2025, as a starting point.

- **WhatsApp**. Because of WhatsApp's popularity throughout the world, many survivors may already use it regularly. Note: While WhatsApp encrypts the *content* of messages and calls, it does not encrypt *metadata* - data about the data, such as contacts lists, who someone calls, and for how long.
- **Signal**. Signal works similarly to WhatsApp, allowing direct messages, groupchats, and calls between Signal users. Unlike WhatsApp, it does encrypt metadata. Also unlike WhatsApp, Signal users can use VoIP numbers (such as from TextNow, MySudo, or Google Voice) to set up accounts. While it is increasing in popularity, it may be less familiar to some survivors than WhatsApp.
- **iMessage**, which is familiar to many iPhone users as a way to send messages, is encrypted. However, both people in the conversation must be using Apple devices in order for the encryption to work.
- **Briar, DittoChat, and Meshtastic**. These apps offer different kinds of *offline* communication, which can be useful if a disaster causes a temporary internet shutdown. To learn more about them, see the earlier section **How can survivors best communicate with local victim service providers during a disaster?**
- **Proton Mail** is one option for encrypted email. Note that in order for end-to-end encryption to work, everyone in the email conversation must be using an encrypted email provider.
    - If this is not feasible, providers can use encrypted email services like Mimecast, in which users have to create a Mimecast account and log into it in order to read emails. With Mimecast, users receive notifications of new messages, with links to access them, in their regular email account.

Different survivors have different concerns and constraints when it comes to the apps they use. Survivors and providers can learn more here: **Choosing and Using Apps: Considerations for Survivors**.

How can survivors and their families keep online accounts secure?

There are certain practices that, while they may not be the right option for every survivor or family, are general digital security "best practice" and may be helpful for many survivors. These include, but are not limited to:

- Multi-factor authentication (MFA) (when you have to provide multiple pieces of information to log into an account or device, such as both a password and a code sent over text).
- Encrypted and/or password-protected messaging platforms. For more information, see the previous section, **Which apps provide encrypted communications?** Learn more about what encryption is and why it matters with Safety Net's **Encryption Basics for Programs** resource.

Additionally, if it is safe for a survivor to do so, they can consider minimizing data sharing and adjusting personal device and application settings. These steps can help to protect privacy, and to reduce the risk if their data or devices are compromised. Learn more with our survivor resources toolkit, **Technology Safety & Privacy: A Toolkit for Survivors**.

How can survivors and their families protect personal devices from spyware/stalkerware and unwanted location sharing?

Spyware/stalkerware is a common concern for survivors. It is important to realize that while stalkerware gets outsized media attention, in many cases of monitoring and location tracking it is not the culprit. Its popularity rises and falls. Cybersecurity company Malwarebytes discusses these trends in detail in a **2023 report on the use of technology to monitor intimate partners**.

However, while its usage has declined since its peak during the height of the COVID-19 pandemic, stalkerware remains a serious problem. And unwanted location sharing more generally is one of the most common ways that abusers misuse tech to monitor survivors. Some options for survivors and their families are:

- Regularly checking personal device permissions. This can help identify unauthorized or suspicious access to location, camera, or microphone.
- Using antivirus software. Antivirus software is essential to protect devices from malware. Many reputable cybersecurity companies offer a free version of their product.
- Avoiding downloading unknown apps.
- Checking devices for rooting and jailbreaking, which are preconditions for installing some types of stalkerware.
- For survivors with iPhones, using the iPhone Safety Check feature, which allows users to quickly review and change a range of security settings in order to block another person's access.
- Survivors with a relatively high level of technical knowledge may consider tools like SpyGuard, a tool that detects potential signs of stalkerware in computer network traffic.

Safety Net has several resources on location tracking:

- Spyware/Stalkerware Overview;
- Survivors' Guide to Location Tracking;
- Tech Talk: Location Tracking: Stalking, Risks and Safety Strategies;
- Connected Cars: Privacy and Safety for Survivors.

6. Personal privacy and public systems

What are the risks to data privacy during disaster situations?

Risks include - but are not limited to - exposure of important data of survivors and their families. This could be through:

- Public networks that might be insecure.
- Exposure of location through apps, IoT devices or vehicles.
- Impersonation of service providers, emergency responders, or legal representatives by abusers.
- Attempts by abusers to claim benefits using a survivor's identity.

How can local victim service providers aid in mitigating the increased risk to survivor's personal privacy during disasters?

It is easier to take steps to mitigate risks ahead of time, than to begin them during a crisis. In this case, mitigating risks refers to reducing the negative impact that an emergency situation could have on the digital safety of survivors and their families. Some ways to prepare might be developing a trauma-informed Incident Response Plan (IRP), providing staff training, setting up emergency communication protocols, and technology safety planning with survivors. You can learn more with Safety Net's Data Security Checklist to Increase Victim Safety & Privacy.

How do emergency response organizations use personal data of survivors and their families during emergencies?

The personal data of survivors and their families could be used for intake, assessment, triage, or coordination of shelter, legal or medical services. Emergency response organizations may collect personally identifiable information (PII) in the process of providing these services. Although access to this information is required to allocate limited emergency response resources, it needs to be encrypted and stored

securely to mitigate cybersecurity risks. Programs can form and maintain relationships with emergency response organizations before a disaster happens, and can advocate with them for strong data security safeguards.

7. What to do if privacy is compromised

How can survivors document abuse if their privacy is compromised?

Documentation of abuse can be discussed with survivors as part of a safety plan. Changes in living situation may require survivors to change documentation tactics. For example, a survivor and abuser being housed in the same shelter, where a survivor may not be able to keep all of their physical devices safeguarded, may necessitate storing more documentation online rather than on the devices. Safety Net's Documentation Tips for Survivors of Technology Abuse & Stalking resource discusses effective documentation, including in the context of safety.

Where can survivors get help if their privacy is compromised?

If survivors' privacy is compromised and they need help, they can call the National Domestic Violence Hotline by dialing 1-800-799-SAFE (7233), texting "START" to 88788, or using the webchat feature thehotline.org. Which method is best will depend on a survivor's needs (for instance, if a survivor's text messages are being monitored, using the webchat with browser privacy tips in mind *could* be a safer option).

There may also be humanitarian workers onsite whose job is to help people who are being affected by, or are at risk for, violence in the post-disaster setting. Some survivors may have opportunities to discreetly ask humanitarian agency staff for help in connecting with these specialists.

8. Tech safety disaster planning

What cybersecurity protocols can organizations implement to ensure continued support during disasters?

Before an emergency situation occurs, organizations should implement cybersecurity protocols that protect survivors, their families, and staff. Confidentiality (preventing those who should not have access to data from being able to access it), integrity (preventing tampering of data), and availability (ensuring that people who should have access to data are able to access it) should be the focus. End-to-end encrypted communication methods, multi-factor authentication (MFA), and role-based access control (RBAC) are all protocols that programs can incorporate. These protocols must consider the specific threat landscape that DV survivors face.

A human-centered risk assessment approach can help to proactively identify, analyze, and mitigate potential security threats to DV survivors. The potential threats may include abusive partners, their family members or friends, and individuals or groups exploiting post-disaster chaos. Protocols need to be reviewed periodically, to make sure that they are up-to-date with the challenges DV survivors and service providers experience.

What should a technology safety plan include?

Technology safety planning should be part of safety planning more generally. Safety Net has guidance on this with the resource Technology Safety Plan: A Toolkit for Survivors. Because disasters may have major effects on a survivor's and their family members' housing circumstances, employment, usual routes for accessing in-person services, technology, and support networks - all of which may have been factors in the safety planning process - the safety plan may need to be modified. Survivors may consider tactics such as disabling

location services, using anonymous browsing, and choosing encrypted communications apps, even if their safety plan did not originally involve those things.

9. Securing emergency technology solutions

How can secure communication be ensured when infrastructure has been compromised?

The most secure options for communication are resilient (able to withstand harsh circumstances) and privacy-preserving. Some options for situations where access to the traditional internet has gone down include: messaging apps with offline capabilities, satellite phones, or mesh networks, all of which are discussed earlier in this document. Training in using these technologies, and switching to them as part of emergency response plans, can potentially be offered to staff during onboarding training and routine in-service/continuing education meetings.

There are many ways that programs can educate and safety plan with survivors and their families regarding disasters. Even small steps like distributing contact cards, emergency phone numbers, and safety instructions, can increase preparedness for both survivors and service providers. If the electricity grid is compromised, ensuring access to backup batteries or solar chargers can help maintain communication when a disaster occurs. Funding for these items can be difficult to find. This is another reason that it can be useful to have relationships with state and local emergency management agencies, as they may have ideas about how programs can obtain them. Outdoors and hiking clubs may have supplies that they would be willing to contribute.

What is the role of technology data backup systems?

If primary systems fail, backup systems such as extra devices, budgeted resources, and virtual backups, ensure data and services remain available and secured. Organizations or their IT providers should implement backup systems as part of their Incident Response Plan (IRP). Backup systems can include:

- Data backups.
- Secured physical copies of files.
- Alternative methods and tools for communication.
- Power sources for devices and locations.
- Services provided by tech companies to ensure "business continuity" to their clients in the event of a disaster.

How can organizations protect data privacy and integrity?

Programs and their IT providers should incorporate survivor-centered, confidentiality-upholding policies and practices into their work, even in ordinary circumstances. Some examples are:

- Data minimization (only collecting the data that a program needs to serve a survivor).
- Encryption throughout the data life cycle. You can learn more about encryption with Safety Net's **resource on encryption basics**.
- Regular review of data collection, retention, and deletion processes.
- Asking for help when needed. Safety Net provides technical assistance (**request form here**) on confidentiality issues. Safety Net's **Confidentiality Toolkit** has extensive resources that may help answer programs' questions.

10. References

1) Bailey, L., Hulley, J., Gomersall, T., Kirkman, G., Gibbs, G., & Jones, A. D. (2023). The networking of abuse: Intimate partner violence and the use of social technologies. *Criminal Justice and Behavior*, *51*(2), 266-285. https://journals.sagepub.com/doi/pdf/10.1177/00938548231206827

2) Bellini, R., Tseng, E., Warford, N., Daffalla, A., Matthews, T., Consolvo, S., ... & Ristenpart, T. (2024, May). Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 635-654). IEEE. https://arxiv.org/pdf/2309.00735

3) Cuomo, D. (2022). Longitudinal reflections on the slow and fast crisis of domestic violence during covid-19. *Area*, *56*(1). https://doi.org/10.1111/area.12829

4) Cuomo, D., & Dolci, N. (2022, May 4). The TECC Clinic: An innovative resource for mitigating technology-enabled coercive control. *Women's Studies International Forum*. https://www.sciencedirect.com/science/article/abs/pii/S0277539522000371

5) Grossman, S., Cooper, Z., Buxton, H., Hendrickson, S., Lewis-O'Connor, A., Stevens, J., Wong, L.-Y., & Bonne, S. (2021, December 20). Trauma-informed care: Recognizing and resisting re-traumatization in health care. *Trauma Surgery & Acute Care Open*. https://pmc.ncbi.nlm.nih.gov/articles/PMC8689164/

6) Hansson, S. (2020, November 2). Communication-related vulnerability to disasters: A heuristic framework. *ScienceDirect*. https://www.sciencedirect.com/science/article/pii/S2212420920314333

7) Houtman, L., Cuomo, D., Dennehy, M., Forman, M., Zea, A., & Hannan, S. (2025). The harm mapping project: Navigating ethics and collaboration in map design. *Cartographic Perspectives*, *(105)*, 27-33.

https://cartographicperspectives.org/index.php/journal/article/download/1943/2399

8) Hubbard, D. W. (2014). *How to measure anything: Finding the value of intangibles in business*. John Wiley & Sons, Inc.

9) Kaspersky. (2023). *The state of stalkerware in 2023*. The Kaspersky Report. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/03/07160820/The-State-of-Stalkerware-in-2023.pdf

10) Kaspersky. (2024). *Is technology making relationships more risky?* [Report]. https://media.kasperskydaily.com/wp-content/uploads/sites/93/2024/09/23151934/ECSM-report.pdf

11) National Institute of Standards and Technology. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication (SP) NIST SP 800-61r3). https://doi.org/10.6028/NIST.SP.800-61r3

12) National Network to End Domestic Violence (NNEDV). (2020). *NNEDV data security*. https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5e288eaf0df7e27ff47264eb/1579716271864/NNEDV_DataSecurity_English08_access.pdf

13) Owen, J. R. (2019, October 12). Catastrophic tailings dam failures and disaster risk disclosure. *International Journal of Disaster Risk Reduction*. https://www.sciencedirect.com/science/article/pii/S2212420919306648

14) Puget Sound Energy. (n.d.). *Energy equity*. PSE. https://www.pse.com/en/about-us/energy-equity

15) Ramjit, L., Dolci, N., Rossi, F., Garcia, R., Ristenpart, T., & Cuomo, D. (2024). Navigating traumatic stress reactions during computer

security interventions. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 2011-2028). https://www.usenix.org/system/files/usenixsecurity24-ramjit.pdf

16) The National Domestic Violence Hotline. (n.d.). *Hotline safetyplan*. Los Angeles Harbor College. https://www.lahc.edu/sites/lahc.edu/files/2022-08/Hotline-safetyplan.pdf

17) The Network/La Red. (2022, August 16). *What is partner abuse?* https://www.tnlr.org/en/what-is-partner-abuse/

18) Thurston, A. M., Stöckl, H., & Ranganathan, M. (2021). Natural hazards, disasters and violence against women and girls: a global mixed-methods systematic review. *BMJ Global Health*, *6*, e004377. https://gh.bmj.com/content/bmjgh/6/4/e004377.full.pdf

19) Washington State Department of Labor & Industries. (n.d.). *Accident prevention program (APP)*. https://www.lni.wa.gov/safety-health/preventing-injuries-illnesses/create-a-safety-program/accident-prevention-program

20) Whitman, M. E., & Mattord, H. J. (2019). *Management of information security* (6th ed.). Cengage Learning.

21) Wisniewska, M. J. (2024, October 7). *Domestic violence statistics 2024*. Break The Cycle. https://www.breakthecycle.org/domestic-violence-statistics/

22) WomensLaw.org. (2024, November 5). *What is nonconsensual image sharing? Is it the same as "revenge porn"?* https://www.womenslaw.org/about-abuse/abuse-using-technology/ways-survivors-use-and-abusers-misuse-technology/abuse-8#:~:text=Nonconsensual%20intimate%20image%20sharing%2C%20abbreviated,or%20videos%20of%20someone%20without