UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Securing Mutual Aid

CYBERSECURITY PRACTICES AND DESIGN PRINCIPLES FOR FINANCIAL TECHNOLOGY

ELIJAH BAUCOM, ANNA LANZINO, YVETTE VARGAS, NICHOLAS PEREMATKO

CLTC WHITE PAPER SERIES

Securing Mutual Aid

CYBERSECURITY PRACTICES AND DESIGN PRINCIPLES FOR FINANCIAL TECHNOLOGY

ELIJAH BAUCOM, ANNA LANZINO, YVETTE VARGAS, NICHOLAS PEREMATKO

October 2025

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Mutual aid organizations, such as food banks, disaster relief, direct cash assistance, and bail funds, serve as critical community pillars, yet their efforts are increasingly under threat in a hostile political landscape, and they often lack the resources to build the necessary digital infrastructure to defend against online attacks.

Recognizing the urgent need for robust cybersecurity, the UC Berkeley Cybersecurity Clinic and Fight for the Future collaborated to create a comprehensive guide aimed at enhancing the cybersecurity practices of mutual aid organizations. Initially intended as a developer guide for a financial technology platform for mutual aids, the project evolved into a best practices guide focused on improving overall cybersecurity and addressing specific financial technology use cases — as well as a checklist for developers who want to serve these crucial community institutions.

Through interviews with six diverse mutual aid organizations, the Cybersecurity Clinic identified common cybersecurity challenges and tailored recommendations to address these issues. This guide outlines best practices for financial technology usage, general cybersecurity enhancements, and design principles for secure mutual aid platforms. By empowering mutual aid groups with practical cybersecurity protocols, we aim to fortify their operations and protect the communities they serve.

KEY TAKEAWAYS FOR MUTUAL AID ORGANIZERS

In the report, we outline tips for mutual aid organizers to enhance their cybersecurity posture based on current practices. Following are key considerations:

- **Limit personal information on accounts**. Mutual aids should avoid linking members' personal bank accounts, credit cards, or personal information (like phone numbers or names) to accounts on payment platforms such as PayPal or Venmo. Instead of using personal payment accounts, consider using a dedicated account that is not directly tied to any specific member's personal information, like a business/organization account, or obtaining a phone for treasurer duties.
- **Be aware of deplatforming.** Deplatforming, when an account or its functions are temporarily or permanently banned by a technology platform, is a common experience for mutual aids, and is often done without reason or explanation. Organizations should diversify their technology platforms to avoid relying on one service.

- **Prioritize using privacy-centered services and understanding privacy settings.** Mutual aids often rely on Big Tech platforms, like Meta's WhatsApp and Google. Our report provides recommendations for harm reduction techniques for organizations relying on Big Tech platforms, and also outlines more private secure alternatives if a mutual aid is interested in migrating. For all platforms, mutual aids should tailor settings for better security, for example by implementing multi-factor authentication.
- **Establish policies for data retention, communication, and other areas to enhance cybersecurity posture.** Mutual aids can establish policies and guidelines for how sensitive and non-sensitive information is communicated, and more broadly how data is stored and retained. Minimizing the amount of data that is collected and stored will better protect the organization.

KEY TAKEAWAYS FOR FINANCIAL TECHNOLOGY DESIGNERS

The final portion of the report outlines design implications for a future payment platform that is aligned with the mission of mutual aids. Following are key takeaways:

- **Build with mutual aids.** Designers should be mission-aligned with mutual aids and cultivate long-term, trust-based partnerships. The design process should include mutual aid community members and adapt based on their feedback.
- **Design for community control and privacy.** Mutual aids are typically grassroots, decentralized, and privacy-conscious. Designers should create technology solutions that consider this structure and provide controls for mutual aids to maintain autonomy over their data. By default, a platform should protect payment data and metadata where possible.
- **Design with deplatforming in mind.** It's likely that mutual aids will face deplatforming. To prepare, designers should enable funds to be routed through multiple payment methods.
- **Design for accessible identity management.** Most mutual aids do not have hierarchy-based roles and technical staff. Designers should make it easy to create organizational accounts that have accessible configuration.
- **Design with built-in security.** Designers should include security measures, like multi-factor authentication and zero-knowledge encryption, by default.
- **Maintain open standards.** A platform designed for mutual aids should be open-source and auditable.
- **Prioritize accessibility.** Designers should prioritize the accessibility of the tools they are building to ensure they are WCAG-compliant and usable.

Introduction and Background

In collaboration with Fight for the Future, the UC Berkeley Cybersecurity Clinic set out to create a developer guide for a financial technology platform tailored to the needs of mutual aid organizations. The guide was to build on the report *Financial Confidentiality in the Age of Digital Surveillance*, commissioned by Fight for the Future and created by Convocation Research + Design, which explored the effectiveness of diverse privacy technologies in safeguarding financial data.[1] However, during our interviews with six mutual aid groups, we recognized a critical gap in current cybersecurity practices within this sector.

For various reasons, many mutual aid organizations have not implemented adequate security measures to protect their technological and financial systems. This leaves their networks, communities, and assets vulnerable to cyber threats. Before we could imagine a better financial technology platform, we needed to establish a stronger foundation by addressing these pressing cybersecurity concerns.

As a result, the focus of this project shifted. Rather than produce a comprehensive developer guide, we turned our attention to creating a best practices guide for the secure use of financial technology — and for cybersecurity broadly — within the context of a mutual aid organization. Based on our findings, we included design principles for developers seeking to create a mission-aligned alternative to current platforms. Our goal is to empower mutual aid organizations to protect their operations and communities by adopting cybersecurity protocols that fit their unique contexts.

As Dean Spade describes in his book *Mutual Aid*, "Mutual aid is collective coordination to meet each other's needs, usually from an awareness that the systems we have in place are not going to meet them. . . . This survival work, when done in conjunction with social movements demanding transformative change, is called mutual aid."[2] Mutual aids serve as critical community pillars, but their work is increasingly under attack as the political landscape changes, and many do not have the resources or time to build the infrastructure to ward off potential digital attacks. Securing mutual aids' digital presence translates to protecting the lives within the mutual aid network and strengthening our communities.

1 *Financial Confidentiality in the Age of Digital Surveillance: An Audit of Current Privacy Technologies Available to Mutual Aid Organizations*. Fight for the Future, 12 Feb. 2025.

2 Spade, Dean. *Mutual Aid: Building Solidarity During This Crisis (and the Next)*. London, Verso, 2020.

To inform this guide, the Cybersecurity Clinic conducted pro bono cybersecurity risk assessments with six mutual aid groups. These organizations represent a range of services within the human rights sector. Each assessment identified the group's key digital threats and provided tailored recommendations for improving digital security.

This guide presents an overview of common issues identified through our interviews and offers practical recommendations to mitigate digital risks. It also includes a section on key design takeaways for developers and technologists seeking to build mission-aligned financial platforms that meet the needs of mutual aid communities.

Note that, while the Cybersecurity Clinic's research covered a range of mutual aid resources, this guide may not fully address your organization's specific needs. Please review it with your own requirements in mind.

ABOUT THE UC BERKELEY CYBERSECURITY CLINIC

The UC Berkeley Cybersecurity Clinic is an interdisciplinary, public-interest digital security clinic within the University of California, Berkeley's Center for Long-Term Cybersecurity. Through a model similar to university clinics in law and medicine, the Clinic trains teams of students to help social-sector organizations build the capabilities they need to proactively defend themselves against malicious governments, powerful corporations, hate groups, and extremists. Read more about the Clinic on our website (https://cltc.berkeley.edu/program/cybersecurity-clinic). If your organization is interested in a pro bono cybersecurity risk assessment, email us at cybersecurityclinic@ischool.berkeley.edu.

REPORT OVERVIEW

This report is divided into two sections:

I. **Best Practices and Tips for Cybersecurity:** This section addresses best practices for using payment platforms, managing and using organizational emails, and securely storing and managing organizational files, followed by tips to enhance overall cybersecurity.

II. **Design Principles for Secure Mutual Aid Platforms:** Based on our interviews and risk assessments, this section outlines key takeaways for the design of financial platforms intended to be used by mutual aid organizations.

Best Practices and Tips for Cybersecurity

BEST PRACTICES FOR USE OF PAYMENT PLATFORMS

Limit Personal Account Information: Mutual aids should avoid linking personal bank accounts, credit cards, or personal information (like phone numbers or names) to financial service accounts. For example, a volunteer's personal Venmo account should not be used for receiving or distributing funds. Having one user's personal financial service account serve as the organization's account invites serious risks, including accounting issues and the risk of disrupting operations in the event that the member who owns the primary payment account leaves without properly offboarding.

Instead, consider using a dedicated account that is not tied to any specific member's personal information. A business phone for a treasurer, or another designated individual at the organization, may be acquired to achieve this. If your organization sets up a work phone, ensure that proper security settings are put in place. Consider using a mobile virtual network operator (MVNO) or VoIP solution, like MySudo,[3] for more affordable cellphone plans.[4] Note that SMS (i.e., text messaging) is not a secure messaging platform, so if you are using the phone's SMS to communicate sensitive information, consider a zero-knowledge encryption alternative like Signal,[5] which ensures that sensitive information remains private and protected from unauthorized access.[6]

Alternatively, if it fits your organization's needs and scale, consider the business version of payment apps, like Venmo Business. Review tax laws in your state and consult your tax advisor to understand if a business account is a good fit for your organization. Also review the payment platform's privacy policies and consider the risks. For example, Venmo's user agreement indicates that they collect and share significant amounts of personal data, and they are able to delete user accounts without warning or reason.

3 https://anonyome.com/individuals/mysudo/

4 Hughes, Alex. "MVNOs: What Are They and What Are the Best Options?" *Tom's Guide*, 16 Mar. 2022, www.tomsguide.com/reference/mvnos-what-are-they-and-what-are-the-best-options.

5 "How To: Use Signal." *Electronic Frontier Foundation*, 26 Mar. 2025, ssd.eff.org/module/how-to-use-signal.

6 "What Does Zero-Knowledge Mean?" *NordLocker*, nordlocker.com/features/zero-knowledge-encryption/.

Prepare for Potential Deplatforming: Many mutual aid organizations experience being deplatformed, when an account or its functions are temporarily or permanently banned by a technology platform[7] (e.g., when Venmo or Paypal freezes a user's account[8]). To mitigate the risk of being deplatformed from a single payment service, consider setting up accounts on multiple platforms (e.g., Venmo, PayPal, Cash App, etc.). This way, if one platform suspends or terminates your account, you can quickly switch to another platform to continue processing transactions without disruption to operations. If you have one particular platform you prefer, you can use the other platforms as secondary or emergency-only accounts that you do not advertise on your website, social media, flyers, etc.

Deplatforming is a risk across all areas, including social media, payment apps, and banks. Consider creating a comprehensive plan that outlines alternative platforms and methods for communication, fundraising, and financial transactions in the event of deplatforming. Ensure that all members are aware of this plan and are trained on how to switch if a service becomes unavailable. Regularly review and update the plan to adapt to changing circumstances.

Cut Out Middlemen: Whenever possible, try to minimize reliance on third-party platforms for fundraising, as they can collect metadata and compromise privacy. For example, while Instagram offers a fundraising feature, using it may expose your financial activities to Meta. Instead, try to go directly through your payment platform. For example, instead of using Instagram's fundraising feature, link supporters directly to your PayPal, Venmo, Zelle, or your organization's preferred platform.

Share Gift Cards Securely: If your organization distributes gift cards, avoid sharing them via SMS links, as this method can be easily intercepted and compromise security. Instead, use secure messaging apps like Signal to share gift card information whenever the technological proficiency of the recipient allows. These platforms offer zero-knowledge encryption, ensuring that sensitive information remains private and protected from unauthorized access. Additionally, Signal is a more reliable way to verify your recipient. In general, we recommend using secure platforms for all of your organization's communications.

Enable Multi-Factor Authentication (MFA): Always enable MFA on payment accounts to add an extra layer of security. This helps protect against unauthorized access. Opt for secure app-

7 "Deplatforming." *Charity & Security Network*, 22 Oct. 2019, charityandsecurity.org/issue-areas/deplatforming/.

8 "22 Rights Groups Tell PayPal and Venmo to Shape up Policies on Account Closures." *Electronic Frontier Foundation*, 15 June 2021, www.eff.org/press/releases/22-rights-groups-tell-paypal-and-venmo-shape-account-freezes-and-closures.

based MFA like Ente Authenticator[9] or Bitwarden Authenticator[10] over SMS-based MFA. SMS-based MFA is not recommended because it puts the user at risk of having their phone number stolen via SIM-swapping attacks,[11] being coerced for information through social engineering,[12] or other types of attacks.

Be Cautious with Payment Notes: When making transactions, avoid including explicit details about the nature of the payment in the notes section. Instead of stating the specific purpose of the transaction, use vague or neutral descriptions to protect the privacy of both the sender and recipient. This helps minimize the risk of sensitive information being exposed or misinterpreted by third parties who may have access to transaction records.

Encourage Cash Donations: If feasible, encourage cash donations for certain transactions to avoid digital tracking altogether.

BEST PRACTICES FOR ORGANIZATIONAL EMAILS

Establishing emails tied to your organizational domain is an important step for any mutual aid. Utilizing organizational email accounts is much safer than using volunteers' personal accounts for organizational affairs, as the latter presents risks such as data loss and hacks. Personal accounts are more susceptible to risks because the mutual aid organization cannot control the volunteer's security settings, like setting a strong password or enabling MFA, or data retention settings, like downloading a volunteer's emails before they are offboarded. Following are recommendations to set up domain-specific emails:

Register the Domain: Use a domain registrar to purchase and register your chosen domain. It is recommended to register all similar domains — like .co, .com, and .org — to protect the organization's reputation and prevent impersonation. Most organizations can use CloudFlare, as this is a widely used platform for registering domains and provides comprehensive services. Further, it is recommended to separate your domain registrar and DNS host to reduce deplatforming risks.[13]

9 ente.io/auth/.

10 bitwarden.com/products/authenticator/.

11 "What Are SIM Swap Attacks, and How Can You Prevent Them?" *1Password*, 15 Nov. 2022, blog.1password.com/what-is-sim-swapping/.

12 "What Is Smishing?" *Cloudflare*, 2022, www.cloudflare.com/learning/access-management/smishing/.

13 "Distinction: Domain Registrar vs. DNS Hosting." *DNS Made Easy*, 30 June 2024, dnsmadeeasy.com/resources/distinction-domain-registrar-vs-dns-hosting. Accessed 24 Sept. 2025.

Select an Email Hosting Provider: Select an email hosting service that fits the needs of the organization. For stronger cybersecurity, it is recommended to use ProtonMail due to its zero-knowledge encryption practices, meaning that Proton cannot read messages or hand them over to third parties. Additionally, it is recommended to assess additional features such as storage space, security, collaboration tools, and customer support.

Set up Email Accounts: Email accounts should be established based on the organization's structure. Consider creating role-based emails for specific functions, such as marketing, fundraising, HR, etc. (for example, treasurer@yourdomain.com or marketing@yourdomain.com). Creating emails based on role or function improves organization and addresses security concerns, ensuring that communications stay in the proper channels and that the personal identities behind organizational roles are kept private.

Implement SPF, DKIM, and DMARC: Set up these email authentication protocols to help prevent spoofing and phishing attacks.[14] Your email provider may provide these additional reinforcements by default; otherwise, consider reaching out to a trusted IT provider or consultant to assist with implementation.

Set up Security Measures: Organizations can enhance security by requiring a second form of verification for account access through two-factor (also called multi-factor) authentication (2FA or MFA). This is an absolute must, especially for accounts that may engage with sensitive information being exchanged (e.g., financial transactions). Organizations should also ensure that emails are set up to detect spam.

Migrate Existing Emails (if applicable): If you are considering moving from a Big Tech email platform to a privacy-focused alternative, develop a plan for how to migrate existing emails, contacts, and calendars. Many email hosting providers offer tools or guides for migrating data from other platforms.

Train your Team: Ensure your team knows how to use the new email system, including features and best practices for security. Develop email usage policies, including professional communication standards and security protocols. Consider running simulations to prepare employees to be cautious about emails, for example by sending simulated phishing emails or messages that mimic real-world attacks.

14 Cloudflare. "What Are DMARC, DKIM, and SPF?" *Cloudflare*, 2023, www.cloudflare.com/learning/email-security/dmarc-dkim-spf/.

Monitor and Maintain: Periodically check user accounts and permissions to ensure they are up to date, and keep up with updates from your email provider regarding new features or security measures.

Backup Emails: Consider using third-party backup solutions to regularly back up your emails and data. Do this on a regular basis and establish archival practices that are aligned with your organization's needs. Prioritize data minimization, which means collecting only the data your organization really needs, and only store it for as long as it is needed.[15] Consider using a solution like Thunderbird.net, a free, open-source, privacy-centered platform for managing and maintaining email. Include a section for backing up emails in a data retention policy to ensure consistent back-up timing and organizational alignment. Make the policy as strict as is viable, and try to back up emails to your local device or onto an external hard drive as frequently as possible.

BEST PRACTICES FOR FILE STORAGE

Many organizations use Google services to handle sensitive information, including financial information. Handling financial or sensitive information on Google Drive requires careful consideration of security and privacy, as Google stores and shares their users' data.[16, 17] However, it is understandable that some organizations may not be able to fully disengage from Google's services. It is not an all-or-nothing situation: there can be an intermixing of Google Drive usage and other secure storage solutions, like OnlyOffice or CryptPad, for highly sensitive information. This section will break down best practices for organizations that wish to use Google services and those that may want to use alternative solutions.

Tips for Continued Use of Google Services

Use Secure Access Controls

- **Limit Access:** Only grant access to individuals who absolutely need it and set a standard policy establishing how and why those individuals should use the platform.

15 "Data Minimization | European Data Protection Supervisor." *EDPS*, 12 Feb. 2024, www.edps.europa.eu/data-protection/data-protection/glossary/d_en.

16 Cyphers, Bennett. "Google Says It Doesn't "Sell" Your Data. Here's How the Company Shares, Monetizes, and Exploits It." *Electronic Frontier Foundation*, 19 Mar. 2020, www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and.

17 Kavenna, Joanna. "Shoshana Zuboff: 'Surveillance Capitalism Is an Assault on Human Autonomy.'" *The Guardian*, 4 Oct. 2019, www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy.

- **Set Permissions:** Use Google Drive's sharing settings to control who can view, comment, or edit files. Regularly review and update permissions.

Enable Two-Factor Authentication (2FA):

- **Require 2FA:** Require all users to enable two-factor authentication on their Google accounts to add an extra layer of security.

Organize Files Properly

- **Use Folders:** Organize sensitive information into specific folders and apply appropriate sharing settings to those folders. As an additional layer, regularly preserve necessary, important files on an external storage device or on your local device and, in especially important cases, make multiple backups in case of data contamination. Only retain files and backups that your organization needs and only retain them for as long as you need them.
- **Naming Conventions:** Use clear and consistent naming conventions to easily identify sensitive files without exposing their content.

Regularly Audit Access and Activity

- **Monitor Activity:** Use Google Drive's activity dashboard to monitor who has accessed or modified files.
- **Conduct Regular Audits:** Periodically review access permissions and file sharing settings to ensure compliance with your organization's policies.

Educate Employees

- **Training Programs:** Provide training on data security best practices, including how to handle sensitive information and recognize phishing attempts.
- **Create Guidelines:** Develop clear guidelines for employees on how to store, share, and manage sensitive information.

Use Google Drive's Security Features

- **Data Loss Prevention (DLP):** Enable data loss prevention, which allows an organization to create rules that control the content that users are able to share outside the organization.[18]
- **Activity Alerts:** Set up alerts to be triggered by unusual activity, such as large file downloads or when users access the Drive from unfamiliar locations.

18 "Use Workspace DLP to Prevent Data Loss - Google Workspace Admin Help." *Google Workspace Admin Help*, support.google.com/a/answer/9646351?hl=en.

Back Up Important Data

- **Regular Backups:** Implement a strategy for backing up critical files stored in Google Drive to prevent data loss, whether on an external hard drive or through local backups to your device.

Be Aware of Compliance Requirements

- **Understand Regulations:** Be aware of any legal or regulatory requirements related to data protection (e.g., GDPR, CCPA, HIPAA) that may apply to your organization. While not all regulations are applicable in the U.S., it is important to recognize existing frameworks that may impact your operations.
- **Data Retention Policies:** Establish and enforce data retention policies to ensure sensitive information is stored and disposed of appropriately. Determine the minimum period for data retention required by law and for your operations, and have a system for purging all information outside that window. Prioritize data minimization, which means collecting only the data your organization really needs and only storing it for as long as it is needed.[19]

Prepare an Incident Response Plan

- **Prepare for Breaches:** Develop an incident response plan to address potential data breaches or security incidents involving sensitive information.
- **Regularly Review the Plan:** Update the plan as necessary and conduct drills to ensure that all employees know their roles in the event of a security incident.

Tips for Alternatives to Google

If an organization prefers not to use Google services for handling financial or sensitive information, there are several alternative cloud storage solutions that offer robust security features. Regardless of the platform chosen, organizations should follow similar best practices for handling financial or sensitive information:

- **Implement Strong Access Controls:** Limit access to sensitive files and regularly review permissions.
- **Enable Two-Factor Authentication:** Use 2FA to enhance account security.
- **Educate Employees:** Provide training on how to securely handle sensitive information.
- **Regularly Audit and Monitor:** Keep track of file access and sharing activities.
- **Back Up Important Data:** Ensure that critical files are backed up regularly.

19 EDPS. "D | European Data Protection Supervisor." www.edps.europa.eu, 12 Feb. 2024, www.edps.europa.eu/data-protection/data-protection/glossary/d_en.

Highlighted Resources for Alternatives to Google

CryptPad and OnlyOffice are both collaborative tools that can serve as alternatives to Google for handling sensitive information, including financial data. Here's how each fits into the landscape of secure document management and collaboration:

CryptPad

CryptPad is an open-source, privacy-focused collaborative platform that allows users to create and share documents, spreadsheets, presentations, forms, and other types of content without compromising on security.

Key Features:

- **Zero-Knowledge Encryption:** CryptPad has built-in zero-knowledge encryption, meaning their servers cannot access your data.
- **Self-Hosting Option:** Organizations can choose to self-host CryptPad, giving them complete control over their data and security.
- **Anonymous Collaboration:** Users can collaborate without needing to create an account, which enhances privacy.
- **Real-Time Collaboration:** CryptPad supports real-time editing and collaboration on documents, similar to Google Docs.
- **Variety of Document Types:** Also similar to Google Docs, CryptPad offers a variety of tools, including text documents, spreadsheets, presentations, and kanban boards (for project management).
- **Open Source:** As an open-source platform, CryptPad allows for transparency and community-driven improvements.

Use Cases: CryptPad is particularly suitable for organizations that do not need a robust office suite but still need ways to securely store documents. Its out-of-the-box encryption and self-hosting option makes it a good candidate for organizations handling sensitive data.

OnlyOffice

OnlyOffice is a comprehensive office suite that provides document editing, project management, and collaboration tools. It can be deployed on-premises or as a cloud service.

Key Features:

- **Document Editing and Collaboration:** OnlyOffice offers document editing capabilities similar to Microsoft Office, with real-time collaboration features.

- **Self-Hosting Option:** Organizations can choose to self-host OnlyOffice, giving them complete control over their data and security.
- **Integration with Other Services:** OnlyOffice can be integrated with various cloud storage services, including Nextcloud and ownCloud, allowing for flexible data management.
- **Document Management:** OnlyOffice includes features for document versioning, access control, and workflow management.
- **Security Features:** The software provides options for encryption, secure access, and compliance with data protection regulations.
- **Compatibility with Microsoft Office:** OnlyOffice is highly compatible with Microsoft Office, making cross-collaboration easy and usage intuitive for Microsoft users.
- **Desktop and mobile applications:** OnlyOffice maintains desktop and mobile applications, making work more seamless and mobile.
- **Open Source:** As an open-source platform, OnlyOffice allows for transparency and community-driven improvements.
- **User-friendly:** OnlyOffice is user-friendly due to its familiar interface, which is similar to Microsoft Office.

Use Cases: OnlyOffice is ideal for organizations that require a robust office suite similar to Microsoft Office with strong collaboration features and the option to self-host for enhanced security. It is suitable for handling sensitive information, especially when organizations want to maintain control over their data infrastructure.

CryptPad vs. OnlyOffice

Both CryptPad and OnlyOffice are valuable open-source alternatives to Google Drive for organizations looking to handle financial or sensitive information securely. As noted above, CryptPad is best for those who prioritize privacy and need a simple, secure way to collaborate in-browser, with more advanced security options for those who wish to self-host. OnlyOffice is suitable for organizations that require a full-featured office suite similar to Microsoft Office with strong collaboration tools and the option for self-hosting, with optional controls over data security. When choosing between these options, organizations should consider their specific needs regarding collaboration, security, and data management.

OVERALL TIPS FOR ENHANCED CYBERSECURITY

Maintain Organizational Structure

While most mutual aid groups operate with a flat organizational model, it is important to maintain some level of management structure for security and overall organizational sustainability.

Define Roles: Clearly outline the responsibilities and expectations for each role within the organization. Depending on your organization, this could entail defining roles for different types of volunteers, employees, and board members; alternatively, it could include differentiating "core members" from "new members" (or some other descriptor). Be specific about the parameters of each role, as this will lay the foundation for delegating individuals' access to digital resources.

Define Access Levels: Based on the defined roles, lay out what documents and accounts each member of the organization needs to access. Limit who has access to sensitive information, such as banking credentials or personally identifiable information. Set up your document drives, password managers, and various accounts in accordance with these roles and access levels. This helps protect the organization from unauthorized access and ensures that only trusted individuals can manage important functions, which in turn protects your community.

Delegate Responsibilities: Distribute tasks and responsibilities among members to prevent overreliance on any single individual. By delegating roles, you not only empower members but also create a system of checks and balances that enhances accountability and reduces the risk of errors or fraud.

Analyze New Services

When evaluating the safety and trustworthiness of a new service, particularly in the financial sector, it is important to conduct a holistic analysis that considers technical, operational, and business risks. Below are key areas to assess:

- **Stakeholders and Investors:** Identify the individuals or organizations behind the service. Investigate their track record, reputation, and previous ventures. Funding sources and key investors can signal credibility, or raise red flags if they have a history of involvement in unethical or unstable projects.

- **Business Model Transparency:** Understand how the service generates revenue. Common models include charging fees, taking a percentage of transactions, or monetizing user data. A clear and honest business model is generally a positive indicator; opaque or overly complex models may signal hidden risks.
- **Data Collection and Sharing Practices:** Review the types of data the service collects and with whom it shares that data. Pay close attention to privacy policies, terms of service, and compliance with regulations like GDPR or CCPA. Consider:
    - Is sensitive data (e.g., financial, biometric) collected?
    - Is data sold to or shared with third parties?
    - Is the data collection proportional to the service being provided?
- **Security and Compliance Posture:** Look into the service's approach to cybersecurity, including encryption practices, authentication methods, and breach history. Determine if the company adheres to relevant financial or data protection regulations.
- **User Reviews and Community Reputation:** Gather feedback from real users and security communities. Early adopters often surface security concerns or unethical behavior. Reviews and other feedback can be found on platforms like Reddit, Trustpilot, and app stores.
- **Third-Party Dependencies:** Determine if the service relies on external vendors or infrastructure (e.g., cloud providers, payment processors). These can introduce additional risk, especially if those third parties lack strong security practices.

Establish Communication Guidelines

Establishing secure and reliable communication practices is essential for minimizing risk, especially when handling sensitive information or coordinating activities. The following principles should guide how teams communicate:

- **Use Encrypted Messaging Services:** When digital communication is required, prioritize zero-knowledge platforms such as Signal. Avoid platforms with questionable privacy practices or weak encryption standards. For example, WhatsApp is not recommended due to its association with Meta (Facebook), its limited protection of metadata (including personal information such as names or location),[20] and the potential for backdoor access by corporate or state actors.

20 "Metadata 102 — What Is Communications Metadata and Why Do We Care about It?" *Freedom of the Press Foundation*, 29 Apr. 2024, freedom.press/digisec/blog/metadata-102/.

- **Prefer In-person Communication When Possible:** Face-to-face meetings remain the most secure form of communication, especially for high-risk or sensitive discussions. Avoid digital communication when it is not necessary.
- **Minimize Social Media Exposure:** Avoid conducting sensitive or strategic discussions through social media platforms. Public or semi-public platforms introduce unnecessary risk. If you need social media for outreach, coordinate this communication separately from your organization's core planning efforts and maintain operational boundaries.
- **Establish a Clear Communication Policy:** Define in advance what tools and channels are to be used for specific types of communication (e.g., planning, urgent alerts, public outreach). This prevents confusion, spoofing, or misinformation from being mistaken as legitimate communication. Within the policy, ensure there is a clear plan in the event of a breach of communication tools. Ensure that all team members know:
    - Which platforms are official;
    - Who is authorized to communicate on behalf of the team; and
    - How to verify messages or sender identity.

Design Principles for Secure Mutual Aid Platforms

The cybersecurity challenges identified through our interviews and risk assessments point to critical gaps in the current infrastructure that many mutual aid organizations rely upon. As such, any future financial platform designed for mutual aid must not only meet functional and compliance standards, but also should align with grassroots values of autonomy, resilience, and privacy by design. In addition, developers of financial platforms for mutual aid must be closely aligned with cybersecurity principles or work closely with cybersecurity professionals. Below are eight design principles that should be reflected in any platform's design:

1. BUILD *WITH* MUTUAL AIDS, NOT FOR

Any platform intended to serve mutual aid organizations must be developed in close partnership with their members. Developers must:

- Cultivate long-term, trust-based relationships with mutual aid organizers.
- Include community members in every phase of the design process.
- Prioritize participatory design practices, including listening sessions, co-design workshops, and community-led governance.
- Be prepared to adapt frequently based on evolving needs and feedback.

2. COMMUNITY CONTROL AND DATA MINIMIZATION

Mutual aid groups are often grassroots, decentralized, and privacy-conscious. A platform should require the least amount of information possible. An ideal platform would:

- Allow pseudonymous or role-based user accounts.
- Avoid selling or sharing user data.
- Offer robust data retention and privacy controls so users can customize what data is collected, stored, and shared and for how long.
- Provide local data storage or self-hosted options for sensitive records.

3. REDUNDANCY AND DEPLATFORMING PREPAREDNESS

Deplatforming from payment systems like PayPal and Venmo is a major risk for mutual aid groups. Future platforms designed for mutual aids should incorporate:

- Built-in redundancy, enabling funds to be routed through multiple payment methods (e.g., ACH, card, cryptocurrency, or cash pickup).
- Exportable transaction data and backup systems to allow easy migration.

4. ACCESSIBLE ORGANIZATIONAL IDENTITY MANAGEMENT

Most mutual aids lack hierarchy or technical staff. A platform should make it easy to:

- Create organizational rather than personal accounts.
- Assign multiple role-based logins (e.g., "Treasurer," "Coordinator") with configurable access levels.
- Include account transfer features for leadership transitions or turnover.

5. BUILT-IN SECURITY FEATURES

Instead of expecting users to configure security themselves, mutual aid platforms should:

- Require app-based multi-factor authentication (MFA) by default.
- Use zero-knowledge encryption for communication and data storage.
- Offer guided onboarding for document permission settings and role-based access.

6. METADATA AND PAYMENT NOTE PROTECTION

Platforms should minimize the amount of metadata exposed through transactions. This could include:

- Removing or auto-redacting payment notes/memos.
- Enabling coded labels for transaction purposes.
- Allowing temporary burner links for one-time transactions or distributions.

7. COOPERATIVE INFRASTRUCTURE AND OPEN STANDARDS

Instead of replicating for-profit fintech structures, platforms for mutual aid should:

- Be open-source and auditable.
- Enable local hosting or data federation to avoid centralized points of failure.
- Offer API integrations with other cooperative tools like CryptPad.
- Support ethical funding models (e.g., sliding scale pricing or community sponsorships).

8. ACCESSIBILITY

Platforms must be usable by everyone. A platform that users cannot navigate, read, or afford to use becomes a barrier. Developers should:

- Follow WCAG accessibility guidelines to support screen readers, high-contrast modes, keyboard navigation, and more.
- Ensure mobile-friendliness and performance on low-end, low-bandwidth, or older devices.
- Use plain language in documentation and interface design; avoid unnecessary technical jargon.
- Include multilingual support.
- Avoid design patterns that may exclude neurodivergent users (e.g., flashing animations, confusing flows, or overly time-sensitive actions).

Conclusion

This guide aims to provide cybersecurity best practices for mutual aid funds with a focus on financial platforms, and provides design recommendations for developers seeking to build a mission-aligned financial platform for mutual aid. The risks faced by mutual aid funds are real, but so is the potential for building systems that reflect the care, trust, and autonomy that define mutual aid work.

These design principles are not meant to prescribe a single solution, but to offer a starting point that is rooted in our interviews and risk assessments of mutual aid funds. Our hope is that this guide contributes to the larger effort of building technology that protects and sustains community organizers as they carry out their essential work.

About the Authors

Anna Lanzino is a recent graduate of the UC Berkeley School of Information's Master of Information Management and Systems (MIMS) program, focusing on technology policy, cybersecurity, and product management. She has worked in the UC Berkeley Cybersecurity Clinic for three semesters as both a consultant and program assistant. Anna works to make cybersecurity accessible for under-resourced organizations and individuals.

Yvette Vargas is a Master of Information Management and Systems graduate from UC Berkeley, specializing in data science, technology law, and policy. She works at the intersection of technology, equity, and public interest, with experience spanning cybersecurity, AI governance, and environmental justice. Yvette works to translate complex technology issues into inclusive policy solutions and ethical data use in vulnerable communities.

Nicholas Perematko is a senior undergraduate in the Industrial Engineering & Operations Research department, studying Analytics at UC Berkeley. Nicholas focuses on cybersecurity and IT, and he serves as the president of UC Berkeley's cybersecurity club, BERKE1337, and as director at the Open Computing Facility, a historical computer lab that brings free and open-source computing to UC Berkeley students.

Elijah Baucom serves as the UC Berkeley Cybersecurity Clinic's Director and instructor of the Clinic Practicum in the School of Information. Elijah is a cybersecurity and privacy technologist, engineer, and activist positioned at the intersection of tech, humanity, liberation, and political education.

Acknowledgments

We would like to thank Fight for the Future and Lia Holland for guiding us through this work and leading the charge in studying mutual aids and financial technology. This project is a direct extension of their commissioning of the report, *Convocation Research + Design's Financial Confidentiality in the Age of Digital Surveillance*.

We would also like to thank all the mutual aid organizations we worked with to obtain this information. Thank you for your dedication to this space.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley