The Development and Maintenance of Digital Security Community Resources and Curricula

Summer 2023

Internews

Infuse Project Team and Laura Vidal

Table of Contents

Introduction

Continued digital attacks against human rights organizations, activists, and journalists remain a global concern. The complex digital security landscape requires technology strategies and resources to consider the lived realities of individuals and groups under threat. Human rights organizations, activists, and journalists depend on external digital security experts for security support and resources. Unfortunately, the demand for these external resources, particularly in high-risk regions, substantially exceeds their availability. This imbalance is compounded by the external resources' varying levels of expertise and whether the resources available align with the needs of those seeking assistance.

Digital rights organizations, NGOs, and digital security experts are beginning to develop sustainable resources and training programs that move beyond specific threats or tool-centric trainings that have predominated the sector. Despite these efforts, there is a scarcity of resources that focus on specialized skills. The existing resources are unevenly distributed and may not prioritize threats targeting the most vulnerable. Moreover, individuals in high-risk regions face hurdles in enhancing their expertise due to limited access to training, language barriers, and nonexistent mentorship opportunities. These gaps underscore a critical need for focused capacity-building and equitable resource distribution in the human rights digital security domain.

In response to the digital security challenges facing vulnerable and high-risk groups and individuals, Internews and its partners are collaborating with the digital protector community to co-develop frameworks to standardize, compile, and localize key areas of specialized digital security knowledge and corresponding learning materials. This report aims to provide some insight into the processes behind the development and maintenance of long-term resources and the communities of digital protectors behind them so that best practices and lessons learned may inform the design and implementation of future and ongoing initiatives.

Methodology

To collect background information and inform this research, Internews conducted a review of already existing digital security resources available online. This involved the analysis of various websites, online documents summarizing digital security curricula, and influential blog posts within the digital security domain. Additionally, Internews monitored online events and discussions within digital security communities to gain insights into current trends and issues. The Internews research team also collected resources (e.g., information security lists, publications, and databases) shared by Internews partners and expert sources in the digital security field and created a detailed table to document and analyze these resources. The table not only highlights the features of these resources but also delves into the process of their creation and the challenges faced by their development teams.

The research team designed and executed a series of interview questions with input and collaboration from both internal and external stakeholders. The team then engaged in semi-guided interviews with seventeen individuals. Interview participants were selected based on their involvement in the creation, long-term maintenance, or active use of key digital security resources, including roles such as content creators, maintainers, and engaged users of these community assets. The interview questions were divided into two main categories: Those regarding (1) creating and collaborating on community resources and (2) using community resources. The interviews touched on a variety of projects but focused specifically on 11 digital security resources[1], some of which were community-owned[2], while others were developed almost entirely by teams within specific organizations. The research team focused on the interviewees' experiences in designing and maintaining community resources—including their successes and challenges. The interview questions also explored strategies for long-term resource sustainability, barriers to community engagement, and how to measure their success and impact effectively.

Following the structured interviews, Internews convened a global gathering of digital security experts and partners in Nairobi, Kenya on July 10-13, 2023. The intent of this gathering was to discuss and validate the work performed over the previous several months, as well as incorporate some learnings into the design of a new community resource. At this gathering, the team collected participant information from several small group breakout discussions. These breakout sessions were designed to gather a diverse array of insights, questions, concerns, and issues from attendees. The positive and critical insights gathered from these breakout discussions informed the findings and recommendations presented in this report.

The findings presented in this report should not be considered as a complete reference for digital security curricula, community experiences, the long-term sustainability of digital security projects, or the

[1] List of resources: Conexión Segura, Conexo - Guide of tools and resources, Convite, Digital Security Helpline Community Resources and Documentation, JOSA - Website and blog, Level Up, Protege.la, SAFETAG, Security Education Companion, Security in a Box, Surveillance Self-Defense

[2] There's a variety of ways in which a resource could be considered 'community owned'. For the purposes of this report –and following some of the cases we observed – a community-owned resource is one that is mostly nourished and maintained by its community of users through feedback and updating work. Community owned resources can start and function with the support of a particular organization or funder but need an important amount of volunteer work to function, which makes their workflow complex, and sometimes difficult to sustain.

lives of the communities behind them. Rather, this report represents an exploration and a listening exercise, informed by individuals who have dedicated themselves to this field and can reflect upon what has worked and what has not.

To maintain confidentiality and respect the privacy of the interviewees, their names will not be published and direct quotes will not be included. This report will refer to specific projects and organizations in some examples where it is needed, but in general, the information presented—especially certain insights—will be attributed to the group of interviewees as a whole.

Discussion and Analysis

Insights on digital security resources, curriculum development, and sustainability

Digital security projects often begin with clearly stated scopes of work only to encounter unforeseen challenges and expanding objectives. While the goal at times is to assign a specific person or team to oversee updating the community-owned resource, the implementation of such an idea has remained elusive. In general, the digital security space tends to lack sufficient resources and, as a result, compromises are frequently made by individuals sacrificing their time and well-being, which often includes their mental health, to fill the gaps.

Most projects focused on resource development benefited from dedicated writing sprints in which the team met specifically to develop a particular project. These projects also benefited from feedback and insights gathered at workshops or global events devoted to digital security and internet freedom. This development process, as well as updating and incorporating feedback, often becomes more challenging than anticipated. Various factors may contribute to this. One common challenge is that the project starts out as being driven by a singular goal but, as it unfolds, unforeseen and new sub-goals complicate both timelines and workflows. This expansion of goals is common and underscores the dynamic nature of digital security projects. Additionally, the creation of certain projects may sometimes inadvertently overlook the contextual nuances of certain user communities –some of which are marked by political upheavals and other material limitations that are difficult to foresee. Addressing these contextual nuances requires additional research, flexibility, and management.

Among the interviewees, the issue of duplication of efforts emerged repeatedly. Many resources were found to be copying or creating similar content without much variation. Some participants suggested that centralizing resources could help address this problem. However, opinions varied regarding the effectiveness of centralization in avoiding duplication. While centralization can make resources easier to find, some groups might still need to recreate resources to meet their needs. Resources that essentially deal with the same broader issue or problem can therefore be remade again and again to fit the needs of particular audiences. Many interviewees noted that this diversity of needs and poor documentation of exactly why resources were duplicated highlights the need for indexing efforts, essentially creating a library with dedicated curators who continuously update content. The idea of having a dedicated person such as an “ombudsman” or a “librarian” responsible for managing the resources was mentioned multiple times.

Creating open and convenient communication pathways from community members can foster healthy feedback channels between the resource and its users, although it can lead to some necessary compromises, such as potential messiness in the information flow or in the updating process. Creating several communication spaces can help, according to one of the research participants. In this case, the trainer created a space on Telegram and Signal to collect tools and answer questions, and unexpectedly opened the door to an active community that to this day shares strategies and keeps important information up to date.

Community contribution

A key source of feedback, identified in most experiences, is the engagement with beneficiaries and trainers through workshops, daily interactions, and dedicated sprints. Some other contributions have emerged through collaborations with teams working on different digital security resources. Challenges arise when it comes to curating and integrating feedback from various sources in the long-term, for example, with emails, comments, community events and conversations with peers.

A recurring observation is that while many people benefit from using the resources, they do not always contribute actively to their improvement, even if the resource openly welcomes feedback. In other cases, exemplified by JOSA[3]—in the case of their blog and other digital security resources they share—and Convite[4], the community is actively involved in the creation and updating process. In some of these cases, the process can become chaotic, or advance at a very slow pace, but it is nonetheless more in tune with the life of the community, whose rhythms can be deeply affected by economic and political struggles. Clarity is also highlighted as an important aspect. Some interviewees expressed their intention to collaborate with specific projects but found it unclear whether the project team was open to accepting new ideas. Establishing a consistent and organized feedback process can be beneficial, as it was learned in the case of LevelUp,[5] where feedback became challenging to handle as the community aspect grew in importance. At the same time, some participants talked about a perceived "call-out culture[6]" within the digital protector community. In some cases, this has translated into harsh feedback and that could have discouraged participation for fear of being shamed or criticized for their questions or suggestions[7].

Measuring Impact

Measuring the impact of online curricula and other digital security resources is challenging. Creators often gauge impact through indicators such as the resource being linked and referred to by others or receiving requests for PDFs and printed materials. In the case of Conexión Segura[8], impact measurement involves tracking website visits, the number of reproductions of the videos, and even responses from the government, which, in some instances, blocked access to recommended tools.

Some creators and users take into consideration other aspects through more general observations. The creators of Convite, for example, see the impact of their work through perceived behavioral change

[3] The Jordan Open Source Association. JOSA, for instance, embraces diverse forms of feedback and levels of collaboration, like having community members provide ideas for articles, instead of taking the task of writing one.

[4] Convite is a project by audio collective Noís Radio that focuses on raising awareness about self-care and collective care, especially for indigenous, cimarronas, and peasant guards in southwestern Colombia.

[5] LevelUp is a global community working to strengthen digital safety and security knowledge and practice. They provide resources, tools, and trainings to help users teach digital security to others.

[6] The “call-out culture” was something mentioned specifically in one interview, and it resonated with insights that appeared in others. It refers to an atmosphere in which making mistakes is badly received or harshly pointed out. As a result, participating in dialogues or asking questions within the community can become a source of stress for fear of being ‘called out’ or shamed.

[7] According to a participant, it is possible that such kinds of harsh responses come as a result of the pressure coming from the high stakes that come with dealing with at-risk groups.

[8] Conexión Segura is an initiative of the non-profit organization Venezuela Inteligente and the project VE Sin Filtro, which seeks to promote the use of digital tools to improve access to information and the response capacity of other organizations, activists, and civil society in general.

among members as well as a feeling of strengthening ties within community through the use and development of their resources[9].

According to most participants, impactful resources consider human and pedagogical aspects and are particularly observant of how adults learn (something that set LevelUp apart when it was created). They emphasize the importance of resources being beautifully designed, written in a clear, inviting, and inclusive manner. Furthermore, emotional attachment to a resource was also seen as an indicator of impact. For instance, Security in a Box[10], being one of the pioneering resources, holds sentimental value within the digital security community as one of the first resources to circulate, and one that was also attractively designed and included a printed version.

Sustainability challenges and successes

Funding remains a critical factor in determining the sustainability of digital security resources. Lack of or ineffective funding can hamper initiatives even when they have a strong community supporting their sustainability and relevance. While community involvement is essential, building and engaging a community can be a challenging and unpredictable, especially if the community in question is not well established. Many resources start well-equipped but struggle with ongoing updates due to a lack of long-term structure or designated experts. In some cases, those responsible for updates were already overwhelmed with multiple tasks and competing priorities. The lack of a strategic approach from the beginning of a project has been identified as a reoccurring problem. This has resulted in an overburdened workload and inadequate support for serving communities in need. Important decisions and pivotal moments often lack careful consideration for long-term implications.

Funders often prioritize measurable results within a short timeframe and may not consider the challenges and hardships faced by communities and teams, including political upheavals. Changing the narrative around resource updates is crucial, according to the interviewees, as securing funding for creating a new resource tends to be easier than securing funding for resource maintenance. In fact, resource maintenance is more likely to build on a community of users already involved and committed to the sustainability of a resource rather than starting out with a brand-new resource that has yet to prove its relevance within the larger digital protector community. While many funders and organizations are willing to support the creation of new resources, convincing them to allocate funds for updating work or creating a project that is aimed to sustain long-term can be challenging. Even projects that have demonstrated their relevance and success eventually encounter sustainability challenges due to lack of funding and appropriate support.

In terms of funding, it is common for a specific organization to provide the initial financial support, effectively becoming the owner of the project, or at least seen as such. There have been discussions around the concept of "central funding," or funding coming from a variety of sources, to

[9] The team does organize interviews after periods of work, but they perceive an impact mostly through overall interactions, the continuity in the participation—as irregular as it may be—and the will of the participants to appropriate the project and contribute to it in ways that resonate culturally with the community (many of the participants contribute with songs, rhymes and other musical genres to the audio pieces focused on digital security. You can hear an example on minute 2:50 of episode 3.

[10] Security in a Box provides guides and tools to help users protect their passwords, communication, phones & computers, internet connection, and files. Security in a Box is also accessible anonymously using the Tor Browser.

"democratize" the process and ensure that resources can last in the long term without being dependent on the demands of a particular funder or organization. Some organizations, like Convite, allocate funds to pay community members who volunteer for updating work. They divide tasks and prioritize completing them promptly, especially when they are not time-consuming. Other organizations use funds from other projects or even their own savings to support capacity building for material updates. However, in both cases, the task continues to have a somewhat precarious quality and counts on a community of experts that are already stretched thin and often under a lot of pressure.

Ownership and community-building

Ownership of digital security projects presents unique challenges. When a project is owned by an organization, there is a dedicated team responsible for its sustainability, but users may not feel a sense of ownership or contribute to its long-term support. On the other hand, when the community is seen as the owner of a project, collaboration protocols can become complicated, and the team in charge of integration and communication with the community can easily become overwhelmed. The question of ownership can also be seen as intertwined with trust. If a well-known organization is seen as the owner, it can inspire confidence in the resources behind the project, but it may also weaken community ties or lead to mistrust—depending on the reputation of the organization among the larger digital security community.

Creating an enthusiastic and engaged community while avoiding exploitation and burnout is essential. Live gatherings, although expensive, can strengthen community ties and contribute to trust-building and the generation of new ideas. JOSA, for example, has found effective ways to engage with its community through local events and gamification[11].

Developing and maintaining digital security resources calls for an alignment of efforts that can grow in different directions as well as initiatives that can integrate insights and issues that may prove difficult to measure. Developing a digital security resource that can be sustainable in the long term with strong community engagement must be flexible and responsive to differing views, priorities, and objectives. These efforts should aim to nourish the community and be open to unexpected changes and timelines while also building a strong base for dedicated leadership to align ideas and initiatives.

[11] JOSA incentivizes community participation by offering perks like VPN accounts and cloud storage in exchange for points earned through collaboration on certain tasks. Additionally, providing a wide variety of ways for community members to contribute can foster engagement.

Conclusion and recommendations

This report examines the complexities of developing sustainable digital security resources for human rights organizations, activists, and journalists. This research, including the interviewee responses and the global convening breakout discussions, highlight the dynamic nature of digital security projects and the crucial role of community engagement. The challenges of funding, community ownership, and the implementation of feedback mechanisms are recurrent themes that show the challenges of sustaining these resources over the long term. This report also brings attention to the often overlooked human and emotional aspects of digital security work that includes impacts on practitioners' mental health and the importance of building trust within communities.

Based on an analysis of the research findings and Internews' experience in digital security capacity building, the following recommendations would generate long-term and lasting impacts on the development and sustainability of digital security resources:

1. Foster Collaborative Funding Models: Encourage the adoption of diversified funding strategies, moving away from single-source funding to a more democratized model. This approach can help mitigate the risks associated with reliance on a single funder and promote long-term sustainability.
2. Strengthen Community Engagement and Ownership: Actively involve user communities in the development and updating of resources. This could be achieved by establishing clear and organized feedback processes and encouraging community contributions, thereby fostering a sense of ownership and commitment to the resources.
3. Prioritize Mental Health and Well-being: Acknowledge and address the mental health challenges faced by individuals involved in digital security projects. Provide support mechanisms that recognize the emotional labor involved and highlight the well-being of those dedicating their time and efforts to these initiatives.
4. Adopt a Strategic Long-term Approach: Develop a strategic framework from the outset of projects, focusing on long-term sustainability. This includes planning for regular updates, maintenance, and the potential expansion of project scopes over time.
5. Centralize and Curate Resources: Establish a centralized library or repository of digital security resources that is managed by a dedicated team. This could streamline access to resources, reduce duplication of efforts, and ensure the relevance and timeliness of the materials.
6. Enhance Impact Measurement: Develop more comprehensive and nuanced methods for assessing the impact of digital security resources. This should go beyond traditional metrics and consider behavioral changes, community engagement levels, and other qualitative indicators. Maintainers of different resources should exchange best practices for impact measurement.
7. Build Resilient Community Networks: Invest in live gatherings and other forms of direct engagement to strengthen community ties. These interactions can be pivotal in building trust, generating new ideas, and sustaining enthusiasm and commitment among community members.

Recommendation for Funders in particular:

Present Funding Opportunities to Tend to Existing Resources: Funding entities interested in the long-term sustainability of quality community resources should consider offering funding opportunities which allow for the ongoing maintenance, curation, and improvement of existing resources, which are more likely to come with existing community support and buy-in.

The advancement of digital security resources for at-risk groups requires a concerted and multifaceted approach that balances the need for strategic planning with the flexibility to adapt to changing circumstances and community needs. By funding and implementing these recommendations, we can work towards creating more effective, sustainable, and community-driven digital security resources.