Peer Verification Systems in Digital Protector Spaces

Summer 2023

Image adapted from original by Byrdyrak, licensed under CC BY-SA 4.0

Internews

Infuse Project Team

Table of Contents

Introduction 2

Methodology 2

Peer Verification & Case Studies 2

Identifying Best Practices & Lessons Learned 4

Indicators of Success 5

Navigating Complexities and Addressing Obstacles 6

Advancing Sustainable Practices 8

Conclusion and Recommendations 8

Introduction

The Infuse project aims to implement a decentralized peer verification framework that complements a structured learning path and badge credentialing scheme. The peer verification framework aims to provide a way for digital protectors, upskilled using Infuse in specific areas of specialized technical expertise, to be verified and vouched for such that digital protectors can be sure that the support they offer to at-risk communities is effective. This report focuses on upskilling and verification programs particularly those used in digital protector spaces, and will capture challenges, models, and best-practices and lessons learned around maintaining a long-term and sustainable skill verification program.

Methodology

This report summarizes and identifies common themes from key informant interviews (KIIs), focus group discussions (FGDs), and desk research conducted between April and June 2023. KIIs were conducted with 12 individuals involved in upskilling programs and talent identification. Most of those interviewed are working on upskilling programming in internet freedom and digital protector spaces. Interviews were also conducted with subject matter experts from other disciplines, including the diving, medical, and rescue fields as a way to compare and contrast their approaches to verification with those of digital protector communities; this report, however, does not delve into the specifics of the approaches used in those fields. Two FGDs were conducted with Internews team members, one with members of the Internet Freedom & Resilience team (four participants) and another with staff from other Internews teams (six participants). Insights from interviews were coded into five categories (defining peer verification, benefits of peer verification, challenges and barriers, best practices and lessons learned – as well as indicators of success, and sustainability) and sub-categorized into numerous themes. Additionally, desk research was conducted on examples of peer verification in several contexts; the findings thereof are incorporated into this report. Following this work, Internews convened a global gathering of digital security experts and partners to discuss and validate the work performed thus far in Nairobi, Kenya in July 2023. A significant component of the convening was creating spaces for meaningful discussions, which were designed to garner a diverse array of insights, questions, concerns, and issues directly from individuals engaged in the practice of digital security. The richness of the discussions and the depth of the insights gathered significantly informed the findings and recommendations presented in this report.

Peer Verification & Case Studies

While the term peer verification is itself quite new, history points towards examples of similar systems, be it medieval guilds or similar professional associations. Desk research on those, however, demonstrated that such associations would frequently focus on the welfare of their members alone rather than benefits to society at large, with a tendency to prioritize protecting members over skills development. Research on more contemporary types of peer verification demonstrated fascinating educational innovations, such as students who would verify each other's lab skills prior to demonstrating them to an instructor. While such an approach has yet to become pedagogically mainstream, early data suggests that it can be an effective complement to hierarchical teaching.

Although many informants in our interviews were unfamiliar with the exact term peer verification, they were well acquainted with and able to speak to the general concept of formal and informal mechanisms for validating another person's or one's own competencies (technical, pedagogical, cultural, personal, etc.). This process is often performed as a safeguard prior to recommending or referring someone's services (and a recommendation can in itself be a way of peer verification), and it is often most useful when working with or referring a person whom one has not worked with.

Many informants discussed the **integral role of networks, reputation, and trust** in their experiences with peer verification. These networks are often made up of friends, colleagues, acquaintances one personally knows, and a broader community. This broader community may include people a digital protector doesn't personally know, but still trusts to a large degree because they occupy similar spaces and know similar people. People go to these networks to ask about the qualifications of others they might potentially work with but do not personally know.

Informants had a differing level of reliance on this broader community, which heavily depends on their role and geography. Many reported that they try to work exclusively with people from within trusted networks and only work with people from outside that circle if they are recommended from within—with this being particularly true when working with at-risk communities. Others were more comfortable accepting recommendations from a broader network, including from those with whom they have fewer personal connections and established trust networks. Despite the stated need for trusted and active networks, circles, and communities in safe verification, many also recognize the inherent downfalls of relying on these (see Navigating Complexities and Addressing Obstacles).

Overwhelmingly, informants reported peer verification, and particularly operating through trusted networks, to be **primarily an informal process**. In the digital security space and other fields, many rely on "whisper networks" to gain insight into others' qualifications and character so they know whom to work with and whom to avoid. Beyond word of mouth, some verify individuals informally by reviewing their written materials (articles, resources, etc.) to understand more about their skills and approaches. This informal approach was seen by some as a contributor of success when it meets the needs of the community. Our research focused on peer verification as an indicator of technical skill alone. Still, informants repeatedly informed us that soft skills are in many cases even more important—a security professional who deeply understands technology can cause harm or discord in a community if they are unable to listen and engage from a positionality of cultural sensitivity.

Informants reported **mixed perspectives regarding the importance of more formal processes of verification**, such as certifications and degrees. Many participants working in digital protector spaces stated that, while certifications and degrees can provide assurance of one's baseline knowledge and can be useful, they are not essential, often not requested, and not the best way of verifying qualifications. Hands-on experience and having a successful track record are more important according to most. This is in part because certification typically demonstrates one's knowledge in particular technical areas and does not verify one's interpersonal and cultural competencies. As cost was identified as a barrier for certifications, the lack of importance placed on these forms of verification potentially provide more opportunity for those who would not be able to afford to obtain formal certification and degrees. This contrasts with experiences of participants in other fields where certification is essential.

Many participants struggled to come up with specific examples of peer verification or verification projects, likely because it often takes place informally. Examples that were shared ranged from formal, such as the (ISC)^2 CISSP certification which requires a minimum of 5 years of professional experience, to less formal communities of practice and member organizations, which verify new members based on references and member consensus. One participant mentioned the PGP model or signing someone else's public key as verification of identity. Another model comes from the CiviCERT community, a group of digital protection organizations who work with at-risk communities. CiviCERT generally invites organizations rather than individuals; member organizations must be nominated and seconded by existing member organizations as well as pass a period of time in which no vetoes are raised. Trust is extended to individuals insofar as they are part of and represent their organizations. This makes it reasonably easy to add new individuals to CiviCERT channels, while posing a barrier to entry for freelance and unaffiliated digital protectors or those who are not well-connected enough to be nominated in the first place.

In contrast to approaches in other fields examined, **the internet freedom community generally, and the digital protector community specifically, do not use a formally defined peer verification approach.** Fields such as medicine and diving rely much more stringently on formal certifications, defined sign-offs from senior practitioners, professional memberships, and continuing education as means of peer verification. The mainstream IT sector also more heavily utilizes formally defined certification systems (such as those offered by (ISC)2, CompTIA, ISACA, and vendor-specific certifications) as well as industry-wide and multi-stakeholder efforts to create frameworks for skills and competencies, such as that of NIST NICE and the European e-Competencies framework. Many of the above fields have a research-based standardization of procedures, built on decades of experience. Digital security for human rights defenders is not just a very new field which lacks such experience but also deals with such a variety of beneficiaries that standardization is hardly easy: while security mitigations (and corresponding technical skills) could be crucial for one group, they might be an impediment for another. Given the rapidly changing threat and technology landscape, there seems to be no easy way to transcribe, research, and standardize all such cases, which means that digital security for human rights defenders relies far more on informal procedures, oral histories, and improvisation than other fields do.

Identifying Best Practices & Lessons Learned

There are many considerations in making peer verification successful but perhaps the most prevalent theme to appear across this study's KIIs and FGDs, regardless of field, is the **need for verifying not only technical skills and knowledge, but also soft skills, cultural competency, and pedagogical prowess**. For verifying in the training space, facilitation and teaching skills are particularly important to look out for, with some informants sharing that they prefer to first see someone facilitating a training or workshop in order to evaluate whether they will implement effective engagements and whether they have deep enough understanding of a skill to teach others. Furthermore, one must verify whether someone is not just skilled at teaching but also interested in doing it. Sometimes, there are people who are referred for having advanced technical abilities, but they lack the other capabilities to effectively work with others, particularly at-risk communities. Beyond pedagogical skills, these capacities include cultural competency, understanding of local contexts, working with people, and being a good ally. These types of attributes can sometimes be verified via reputation, and at least one informant pointed out that an effective peer verification framework must not just focus on promoting the technically competent but also flag up those who could become malicious actors. Some informants even would prioritize these types of skills over technical skills with one stating, “with interest, the hard tech skills are learnable by people with the solid ‘soft’ skills.”

Even when working within a trusted network, one still needs to be strategic when picking people from whom they receive recommendations or feedback on referrals. It is critical to get feedback from the specific communities that the person being verified has worked with in the past, while also gathering insight from the community which will be impacted by the referral. Regional and local partners are great resources for this. Gathering this feedback can help in determining the exact needs of a community which will inform the appropriate people to refer. Additionally, informants reported that feedback from trusted individuals with similar skill sets to those being verified can be critical.

Some informants from the digital protector space highlighted the **benefits of in-person engagements**, such as conferences and trainings or shared activities, for verifying competencies and developing trust. This is in part because such engagements allow for more in-depth discussion, foster relationship building, and signal someone’s seriousness in terms of digital protection work. In-person events were noted as key in facilitating networking and regional cooperation, perhaps allowing the trusted networks to grow and include new people; however, in-person engagements can also exclude certain people from these opportunities due to language, financial, and time barriers (see the section below on Navigating Complexities and Addressing Obstacles).

Mentorship was identified by many as beneficial for developing capacity, validating knowledge, and identifying personal gaps in expertise. Mentorship was mentioned by some as being formal, for instance through official programming, and by others as informal, “based on chemistry and connections.” It can also change dynamics over time, starting on a more formal basis and evolving into a more informal relationship. In general, those interviewed called for more opportunities for both formal and informal mentoring.

Indicators of Success

When asked what indicators of successful peer verification processes are, informants shared some of the following:

- At-risk communities are able to connect with verified digital protectors, who are able to provide relevant and effective support
- Members of communities which have some sort of peer verification network engage with the community in a way that demonstrates understanding and respect of community dynamics
- The peer verification network is able to remove individuals who cause harm

- Participants of a peer verification network are able to share knowledge with others both within and outside the network
- Participants of a peer verification network are able to grow professionally and gain skills
- The community itself grows with new members joining, attracted by the opportunity to learn, be validated, and implement skills, for personal or professional reasons

Navigating Complexities and Addressing Obstacles

Although trusted networks were identified by informants as a key component of peer verification in the digital protector space, they also inherently, and arguably necessarily**, foster exclusionary practices** and cultures and distrust of outsiders. Some potentially great contributors may not even know about the networks or have the means to enter. These networks can be exclusionary spaces for those who are deemed to not have the technical skills, with some people self-selecting out of the community due to being intimidated by technological areas and others being rejected from spaces for supposedly lacking a particular level of technical expertise. People of marginalized backgrounds are particularly susceptible to this exclusion, with one informant emphasizing the struggles of integrating members of the LGBTQIA+ community. Women also are underrepresented in peer verification systems. Some people may be excluded from these networks if they are perceived to lack 'necessary' people skills, which could be a barrier to persons with disabilities. People who aren't involved in an organization or unaffiliated may also be excluded from these spaces, despite their possible contributions. There is a struggle to balance inclusivity, which could enrich and improve such networks, with safety, as there is higher risk of misplacing trust the larger the network grows.

Another specific area of exclusion is tied to language. Some informants noted that the **dominance of English in the digital protector space limits access to expertise, events, workshops, etc. for non-English speakers**. This can exclude people entirely from the space or limit them to only participating in regional activities and networks. Furthermore, some organizations struggle to find trainers who effectively can engage in local languages and provide support using language that beneficiaries understand. These issues both make it difficult for diverse language speakers to learn skills and join networks that allow them to be verified (and thus referred to opportunities) as well as for communities to be referred effective support in their language. Expanding networks and mentorship opportunities for non-English speakers would help ensure that language is not a barrier to reaching one's full potential in the digital security space. This would have a ripple effect that empowers individuals to contribute to this global space of skill and knowledge sharing.

Peer verification carries a weight of responsibility. Recommending a person or team creates a chain of trust. If this recommendation turns out to be misplaced or creates negative results, there are serious consequences to consider. Not only does the receiving organization have to navigate the fallout created by the actor, but the recommending organization must consider how this situation questions their judgement and trust in future recommendations. Therefore, its critical to evaluate the importance of endorsements to help ensure trust is well-founded and maintained. Moreover, it is important to continually verify an individual's skill, as one respondent we interviewed emphasized. Individuals in this process should not believe that once verified, this verification will last forever. Continual improvement and learning is important to maintain peer verification long-term.

‘Bad actors’ or community members who cause harm can also create a toxic culture which discourages participation in peer verification networks. Informants shared some of the signs of a toxic actor: taking credit for others’ work, committing violence against women, being a bad educator, and displaying inappropriate behavior in a teaching setting. Unfortunately, some of these actors are often popular or hold important community roles, making it more difficult to raise flags about their behavior or remove them from the community.

Informants determined that in order to encourage the inclusion of diverse voices in digital protector peer verification networks, the community needs to tackle problematic behavior and bad actors and encourage the “loudest” voices to make space for others. They also proposed more intentional relationship-building across movements to help with peer verification by proxy to bring in new people even if direct trust relationships don’t yet exist.

Lack of resources for peer verification, including funding and time, as well as a **mismatch between donor and community priorities**, were raised as additional challenges. Part of this lack of funding is due to funders typically not seeing the value in funding activities focused on networking alone even though networks developed allow for critical work later on.

Peer verification must also consider the disparity of skill levels along with an individual’s self-perception of their own skills. Some people may perceive themselves at the same or higher skill level than their peers, which ultimately, questions the validity of the peer verification process. Individuals may choose not to participate, question the process, its validity, or its reputation. Another challenge with peer verification and learning paths lies in accommodating both beginners and advanced participants. As noted earlier, gatekeeping may be an issue in peer verification. One interviewee noted that one solution is to verify teams—not individuals. They explained the shift of focus from individuals to teams may prevent the search for “unicorns.”

Even when a digital protector is peer verified there is a chance that the assessment will be inaccurate, potentially leading to, at best, ineffective outcomes or, at worst, harmful ones. One challenge is evaluating one’s capacity over time, as some areas of expertise can quickly become out of date. For this reason, it is important to check how recent a potential referral’s contributions are. Furthermore, reputation, which is often a consideration in informal peer verification, can be misleading. There could be in-group bias or tendencies to overestimate the capabilities of “rock star names” within a network.

Our research, along with informant feedback, underscored the importance of creating feasible and accessible methods to evaluate and measure peer verification. Addressing how to do so, however, proved challenging. This gap further highlights the necessity of creating a methodology for measuring the effectiveness of peer verification beyond the badge/learning path framework. It is furthermore essential to be flexible in peer verification initiatives to account for drastically different contexts and threats is essential. This becomes especially important as we consider rapid changes in technology and the diverse legal and political environments in which these peer verification initiatives operate. Therefore, ongoing research and development are imperative to establish reliable, and adaptable, peer verification assessments.

Advancing Sustainable Practices

Keeping a peer verification system active and valuable in the long term, particularly when it was started through limited-time institutionalized funding, is challenging. Informants shared that some degree of recurring funding is likely necessary for upkeep. Such funding is critical for compensating skilled community builders and contributors, whose work is necessary but not always obvious. Some approach the unpredictability of funding by embracing either the nonpermanent nature or the ‘ebb and flow’ of a network by **flexibly adjusting activities and level of work based on whether there is funding at a particular time**. For more informal networks, low maintenance and low-cost mechanisms can also be effective, such as active Signal and Mattermost groups. However, for formal peer verification systems, **governance structures and predictable processes for determining leadership and decision-making** can be effective if there are resources and committed members involved.

Sustainable peer verification networks must also provide ongoing value, preferably for minimal time invested by members, in order for people to stay involved. Social connections and a shared cause are major motivations for many and can be as or more important than professional connections and opportunities. Professional and learning materials, opportunities, and networks can also be strong motivators as well as methods to recruit new members.

Conclusion and Recommendations

The following recommendations for maximizing the quality of peer verification initiatives are based on the findings from this research:

1. Incorporate flexibility into any peer verification initiatives (do not be rigid in standardization) in acknowledgement that security threats and appropriate mitigations for those will vary drastically by context and situation, also given rapid changes in technology landscape and operating legal, political environments.
2. Ensure that there is emphasis not only on verifying technical skills but also interpersonal, intercultural, and pedagogical skills.
3. Foster opportunity for in-person engagement. This is helpful for verifying competencies of others and building trust. These engagements need to be made inclusive in terms of language, financial capacity, time, etc. Funders should invest more in these opportunities and making them accessible.
4. Provide more opportunity to create formal and informal connections between mentors and mentees.
5. More research and work should be done to explore ways to measure effective and inclusive peer verification.
6. More research and work should be done to investigate how peer verification efforts can account for the rapid changes in technological and contextual knowledge and whether those who are verified are updating their own knowledge accordingly.

7. Foster more networks and provide more mentorship opportunities for non-English speakers and expand beyond regional opportunities.
8. There needs to be more intentionality about inclusively welcoming individuals from marginalized backgrounds and without organizational affiliations into spaces where peer verification is happening.

Whether it is done formally or informally (or even unintentionally), peer verification is happening in many ways within digital protector spaces and has implications on the makeup and safety of the digital protector community and the wellbeing of individuals within the community and those receiving support from it. Keeping this in mind, it is worth investing in further discussion and research to identify ways to make these verification systems more beneficial for digital protectors and those they support.