Background Note

Enabling Safe Access to Digital Spaces

Introduction

UNHCR's Digital Inclusion Programme recognizes the right that refugees and other forcibly displaced populations have to actively participate in the current digital revolution. Humanitarian contexts further deteriorated by the COVID-19 pandemic have highlighted the critical importance of a connected refugee community that can efficiently access vital information and life-saving protection services remotely.

However, in addition to these opportunities, facilitating digital access and inclusion of forcibly displaced persons and their hosting communities can inadvertently bring risks for individuals. Whether instances of online fraud, misuse of refugees' data that is captured as they connect or tracing activity on social media, these risks need to be understood, managed and mitigated where possible. Furthermore, having the right skills and systems to safely engage online is paramount for UNHCR's Persons of Concern (PoCs) to ensure they can confidently use available digital tools to increase their resilience. Linked with recent work by the ICRC exploring data protection risks in connectivity interventions, UNHCR is keen to understand more about how these risks manifest and what actions can be taken to minimize the risks faced by communities that occur as a result of their digital access. An initial exploration of the topic has been undertaken in the Connecting With Confidence: Managing Digital Risk report that further frames some of the relevant issues at hand and highlights experience of PoCs across two country contexts (Uganda and Kenya):

Context

Digital literacy is vital to ensuring that individuals can safely, effectively and efficiently use technology. Lack of relevant digital skills and knowledge remains among the main barriers to accessing connectivity services worldwide. In an age where societies as a whole are digitizing rapidly and humanitarian assistance is increasingly being provided through remote digital channels, the importance of addressing this skills gap is vital in ensuring communities are able to navigate often new and unfamiliar digital engagements. Furthermore, data literacy is specifically important as community members not only understand the systems and platforms they're using, but what happens to the data they're generating or providing, how this is processed and by whom. Critically, there are also different ways of addressing such challenges ranging from more top-down 'campaigns' to bottom-up community-driven approaches to enhancing understanding.

Risks do not end with a digitally and data literate population. Other possible risks span across a variety of areas such as:

1. **Secure Connections:** The majority of connectivity accessed by refugees or forcibly displaced persons is provided through cellular connections operated by Mobile Network Operators. In certain contexts however, connectivity is provided through WiFi hotspots, connected community centres and other local solutions. The specific nature of these connections can lead to risks: Is any content filtering in place? How long is data retained for when refugees are using hotspots? Are these local networks secure or vulnerable to attacks? How are such centres governed and by whom? Simple measures can be taken to manage security risks to local network infrastructure;
2. **Digital Surveillance:** How is personal information being used online - consciously or unconsciously? How might third parties monitor, record and use a population's digital footprint and online behaviour? How aware are PoCs about this and how it could affect them in the future when seeking support or solutions?
3. **Securing Access:** Online accounts and personal devices contain valuable personal information but often these are not protected adequately, for example passwords or account information being shared without necessarily understanding the risks. Being aware of how to manage passwords, security and privacy settings, and the broader implications of sharing access credentials for either connections or services is vital to minimize chance of illegitimate access;
4. **Cybercrime:** Can take various forms like online identity theft, financial fraud, stalking, bullying, hacking, email spoofing, information piracy and forgery and intellectual property;
5. **Online Abuse and Sexual Gender-Based Violence:** Social media channels such as Facebook and Instagram have been used as a means of facilitating human trafficking, grooming and sexual exploitation (e.g., by connecting with potential victims through false job advertising or befriending children). In addition, the rampant use of digital technology has led to an increase in online harassment, or unsolicited sexual interactions particularly impacting women and girls.

Scope and objectives

The main objective of this challenge is to build on previous efforts by humanitarian and partner organizations in this space and to ensure sustainable access to connectivity for refugees and their hosting communities to address real and perceived digital risks and guarantee a safe, inclusive and responsible engagement online - considering specific risks and barriers faced by different groups based on age, gender or demographic.

Application

The interventions proposed aim to address online risks faced by affected communities in a given operational context by enhancing their digital skills. Interventions will:

1. Raise awareness about the real and perceived online risks, including the most pertinent risks and targeted specific groups among refugees and other vulnerable populations in accessible formats;
2. Provide the tools for a safer engagement online, safeguarding individual's identity, identifying key information to protect and sharing personal data in a responsible manner;
3. Develop protocols for staff, partners and persons of concern to be able to detect possible online threats and how to efficiently respond to those or refer appropriately.

To submit an Expression of Interest to this challenge click the Apply Now button.
(*You will need to login to your UNHCR account*)

APPLY NOW