Monitoring and Evaluation for Digital Security Training

Prepared by: Kate Long and Ellie Cole

25 X25

Internews


X25
X25

25X25 Series

Internews is an international non-profit that supports independent media in 100 countries — from radio stations in refugee camps, to hyper-local news outlets, to filmmakers and technologists. We train journalists and digital rights activists, tackle disinformation, and offer business expertise to help media outlets thrive financially. For nearly 40 years, we have helped partners reach millions of people with trustworthy information that saves lives, improves livelihoods, and holds institutions accountable.

We commissioned this research as part of the 25 x 25 initiative, our strategic commitment to increase robust evaluation of our work by delivering 25 research studies by 2025. We have made this commitment because we want to know which of our approaches are most effective in order to bring them to scale, to strengthen our understanding of the impact for communities when their information environments improve over time, to make our contribution to the global evidence base, and to hold ourselves accountable to the people we serve.

We produced this report because we saw a gap: digital security training is an increasingly important part of the support provided to journalists and human rights defenders, yet lacks a coherent framework for assessing effectiveness. Through this work, we have produced a universally applicable monitoring and evaluation framework that can be used whenever digital security training is conducted with any audience, and which will ultimately improve the quality of data and evidence available to support the design, development and delivery of digital security curricula which enable at-risk groups to continue their important work safely.

June 2023

About the Lead Researchers

Kate Long is a freelance consultant who specializes in program development and evaluation. She has extensive international experience, having supported youth digital programs in Malaysia, development efforts in Syria, girls' education project proposals in Nepal, and fundraising for Turkish CSOs.

Ellie Cole is a researcher focusing on health and disability in middle and lower-income countries. She is currently a PhD candidate at UCL in London, exploring how people with disabilities in Liberia experience the Covid-19 pandemic and contrasting it with the 2014-2015 Ebola outbreak. She has published extensively on disability and poverty reduction. Ellie works closely with UN agencies, international organizations, academic groups, and civil society organizations.

Kate and Ellie served as the lead researchers for this study.

Acknowledgements

Internews and the lead researchers would like to thank the following people for their contributions to this report:

The regional research team: Ali Sibai, Cecilia Maundu, Chinmayi SK, Fabian Ziffzer and Łukasz Król, who co-designed and tested the research tools, and conducted the research in challenging conditions. This study would not have been possible without their in-depth understanding of local contexts, and their wealth of experience and expertise.

Okthanks and Superbloom, whose report "Understanding Support for the Frontline"[1] laid the foundations for this study, and whose insights and advice have been invaluable. Okthanks developed the Star Measurement Framework informed by the findings of this research filling an important resource gap in the internet freedom community.

The digital security trainers and training participants who took part in focus group discussions, online surveys and interviews. We particularly respect the dedication to excellence, inclusion and learning demonstrated by the trainers who contributed to this study.

Amelia Ayoob, Ashley Fowler and Megan Guidrey of Internews, whose commitment to understanding and prioritizing the needs of both trainers and participants underpins this document. Lorna Fray was the copy editor.

List of Tables and Figures

List of Abbreviations, Acronyms and Definitions

CEE	Central and Eastern Europe
Digital security	The ability to prepare for, prevent, identify, investigate, and/or obtain remedy for repressive digital attacks or other types of repression (including online surveillance and censorship) designed to prevent individuals or communities from exercising their human rights and fundamental freedoms online.
Training Participants	Individuals who have received training on digital security. This includes journalists, academics, human rights defenders, civil society leaders, activists and others working towards societal and/or legislative change. They may work alone, or as part of formal or informal groups or organizations.
FGD	Focus group discussion (this term is also used as shorthand for other forms of in-depth, qualitative responses to this study, including interviews and correspondence)
KII	Key informant interview
LAC	Latin America and the Caribbean
M&E	Monitoring and evaluation
MENA	The Middle East and North Africa
SSA	Sub-Saharan Africa
Trainers	Individuals who provide training and support on digital security to participants.

Table of Contents

Executive Summary

About this Report

Digital attacks (including account takeovers, phishing/spear-phishing, website hacks, DDoS attacks, and malware-related incidents) against human rights defenders, activists, journalists, and other at-risk groups are on the rise worldwide, and only getting more sophisticated.[2] According to Freedom on the Net 2022,[3] digital repression is on the rise, especially in authoritarian countries. Under increasing attack, people need support to make necessary improvements to increase their digital resiliency.

Internews partners with local digital security experts around the world to train at-risk groups to help make them safer online. The goal of Internews' digital security programming is to improve the ability of these groups to prepare for, prevent, identify, investigate, and/or respond to repressive digital attacks or other types of repression (including online surveillance and censorship) which are designed to prevent them from exercising their human rights and fundamental freedoms online and conducting their work.

Given that trainings often take place in complex or even dangerous environments, and that accessing training can draw unwanted attention to trainees, Internews relies on local trainers who serve as trusted intermediaries. Their in-depth understanding of the context and deep trusting relationships allow them to effectively and covertly provide the digital security support needed most by at-risk groups. However, local trainers often lack strong evidence or frameworks for understanding the effectiveness of this support.

This report covers a 2021 research study commissioned by Internews to, firstly, understand the challenges faced by digital security trainers in measuring the efficacy of training — an area where they are under-resourced and lack global standards — and, secondly, to assess the factors preventing or enabling trainees ('participants') around the world from applying what they learn. Following the research study, the lead researchers and collaborators on this report used the findings to create a measurement framework for digital security training that includes a complete suite of resources: recommended indicators, corresponding measurement methods, and data collections tools, along with guidance on how to deploy these resources alongside any digital security training.

The findings and recommendations in this report, and the measurement framework it

inspired, may apply to digital security training delivered by organizations beyond Internews. The measurement framework fills a gap in the sector by identifying tangible ways to help trainers measure the impact of digital security training through standard indicators and easy to use data collection tools and templates.

Methodology

Research Design

Building on 2020 research,[4] this study was designed by Okthanks, Superbloom, Internews, and lead researchers Kate Long and Ellie Cole, to assess:

- Challenges digital security trainers face in measuring the efficacy of their training
- Resources they need to do this
- Barriers preventing participants from applying learning acquired through digital security training

The lead researchers devised a training impact model comprising four aspects: experience, learning, application, and impact (see **Figure 1**), which formed the basis of an initial measurement framework.

Research Sample, Data Collection and Limitations

Internews recruited five regional researchers to implement the study — one each for Latin America and the Caribbean (LAC), Sub-Saharan Africa (SSA), the Middle East and North Africa (MENA), Central and Eastern Europe (CEE), and Asia. Unfortunately, the MENA researcher was unable to complete the study and there was not sufficient time to recruit and onboard a replacement during the limited scope of the study.

The mixed-method study gathered qualitative and quantitative data through separate online survey questionnaires for digital security trainers and training participants, and separate online or in-person focus group discussions (FGDs) with trainers and training participants. To overcome low response rates, researchers invited research contributions via key informant interviews (KIIs) or correspondence.[5]

The respondents to this study are journalists, activists, academics, human rights defenders, civil society leaders, and digital security trainers. Overall, 79 trainers and 43 participants completed questionnaires, and 47 trainers and 40 participants engaged in discussions

(see **Table 1**). These respondents represented all regions except MENA, particularly LAC and SSA. By taking part, these people were arguably demonstrating a positive attitude towards digital security training.

Key Findings Relating to Digital Security Training

All but one FGD participant (trainees) viewed digital security as overwhelming and mysterious, and many perceived digital security training as a necessary chore in order to pursue their 'real' work.

Accessing Training: Barriers and Enablers

Factors that prompt people to access digital security training:

- Understanding the specific digital security risks they face, and that training can enable them to avoid or reduce those risks
- A recommendation from someone they know who has attended similar training

In all regions, participants emphasized the importance of trust when searching for a digital security trainer — most used their personal networks to identify trainers. This works well for people who are part of digital security or Internet freedom communities but may exclude others.

Across all regions, participants wanted trainers with digital security expertise that they can relate to their real-life work and context. With a few exceptions, participants were unconcerned about trainers' gender, age, nationality or ethnicity.

None of the trainers interviewed or surveyed reported directly charging participants for their training. Free access to training may reinforce participants' perceptions that investing in digital security is not important.

Issues that Affect Training Quality and Application of Learning from Training

The vast majority of trainers find training resources online, and tailor them to their own language and context, as many resources originate from the US or Europe. Trainers felt that short-term funding limits the time and resources they can use to research and develop

new materials or approaches. Short-term funding also reduces follow-up with trainees, to ensure that their learning is embedded and applied.

Almost all training participant survey respondents (93 percent) reported they applied at least some of the learning and tools they received from digital security training. The most commonly reported enabler of this was the practical nature of the training: 53 percent of these respondents mentioned the importance of having time to practice new skills during training sessions, being able to ask questions and apply the training to everyday scenarios.

For those who had not applied the skills and tools acquired via their training, the main reasons were limited Internet connectivity and access to digital devices. Internet connectivity was particularly challenging in SSA and LAC, and to some extent in rural Asia.

However, a large minority (41 percent) of surveyed training participants who had not implemented skills gained during their training said they needed more input from the trainer.

The Need for Ongoing Support

The findings highlighted two distinct approaches to digital security training: short-term, one-off sessions versus longer-term, ongoing support. The short-term model is most common in SSA and Asia, while ongoing support is beginning to dominate in CEE and LAC.

While trainers from all regions believed that short-term training is still valuable, especially to support participants on a single, specific issue, several findings underline participants' need for ongoing digital security support. Both trainers and training participants recognized that behavior change can take time. And 10 percent of training participant survey respondents mentioned the importance of support and buy-in from colleagues in applying skills and tools acquired from training, emphasizing the importance of ongoing support for organizations and communities as well as individuals.

Already, 85 percent of trainer survey respondents reported doing more than delivering training. A large minority of these (39 percent) provide ongoing technical support (see **Figure 2**), sometimes in response to ad hoc requests. While these ongoing relationships help trainers to understand participants' needs and the impact of their training, ongoing support is very rarely paid for by participants and not always covered by external funding. Particularly in SSA and Asia, a reluctance to place further unpaid demands on trainers is the most significant factor deterring participants from engaging with trainers in the long term.

Digital Security Training Measurement Framework

The research findings confirmed the logic of the experience, learning, application, and impact model (see **Figure 1**), and led to a simple theory of change: *if* participants learn how to improve their digital security, and *if* they implement that learning, *then* they will be less likely to experience the negative impacts of digital threats. To help apply this practically, the lead researchers devised an initial digital security training measurement framework that Internews is now refining and piloting in its digital security training programs. The framework includes various draft indicators to measure the experience, learning, application, and impact of digital security training are explained starting on page x.

Key Recommendations Relating to Digital Security Training

Conduct Additional Research and Testing

1. Conduct research in MENA, perhaps reusing this study's tools or inviting comment on this report/the measurement framework
2. Schedule future research over a longer period, and perhaps use third parties as well as Internews-affiliated regional researchers to recruit research participants and/or host FGDs/KIIs
3. Commission an independent observer to assess digital security training sessions, or assess trainees' learning in future project evaluations
4. Continue asking trainers and participants about the enablers of, and barriers to, applying learning from training, perhaps through a question in narrative reports or informal conversations
5. Test the framework to measure digital security training with people who have not been involved in this study

Develop Additional Training Materials

1. Fund the development of Global South-led, high-quality, accurate, up-to-date and accessible training materials that can be widely used, adapted and shared
2. Support the development of a simple training curriculum by experienced trainers in the Global South, to include key stages for each core topic

Make Training More Accessible and Inclusive

1. Work with trainers to create awareness-raising and recruitment materials for a range of audiences, including relevant statistics and case studies
2. Explore ways of using trainee cohorts to recruit new participants
3. Approach potential training participants from outside the Internet freedom community
4. Ask trainers to provide participant data that is disaggregated by gender, age, disability, etc.

Invest Effectively in Training

1. Consider funding to broaden access to the Internet, digital devices and software
2. Recognize the time involved in preparing training and any follow-up (not just training delivery), and consider increasing funding for ongoing training support

Introduction

The Purpose of this Report

This report covers a research study initiated by Internews to better understand the challenges faced by digital security trainers in measuring the efficacy of training — an area where they are under-resourced and lack global standards, and factors preventing or enabling trainees ('participants') around the world from applying what they learn. The lead researchers and collaborators on this report used the research findings to develop a measurement framework for digital security training that includes a complete suite of resources: recommended indicators, corresponding measurement methods, and data collections tools, along with guidance on how to deploy these resources alongside any digital security training.

The findings and recommendations in this report, and the measurement framework it inspired, may apply to digital security training delivered by organizations beyond Internews. The measurement framework fills a gap in the sector by identifying tangible ways to help trainers measure the impact of digital security training through standard indicators and easy to use data collection tools and templates.

Background to this Report

Digital attacks (including account takeovers, phishing/spear-phishing, website hacks, DDoS attacks, and malware-related incidents) against human rights defenders, activists, journalists, and other at-risk groups are on the rise worldwide, and only getting more sophisticated.[6] Around the world, Internews regularly partners with local digital security experts to train at-risk groups with the goal of making individuals and communities safer online. At-risk groups need to be able to prepare for, prevent, identify, investigate, and/or respond to these increasing repressive digital attacks or other types of repression (including online surveillance and censorship) which are designed to prevent them from exercising their human rights and fundamental freedoms online.

Supporting local trainers who better understand the context-specific digital security risks may reduce the risk to participants and improve outcomes of these trainings. However, relying on trainers as intermediaries limits a funder's direct access to participants and this approach requires trainers to directly collect evidence that their training increases security knowledge and encourages more secure online behavior.

Based on qualitative data and informal feedback collection over a number of years, it is clear that impact measurement is an area where trainers are under-resourced or lack the support they need. In addition, there are currently no globalized standards for measuring the impact of digital security training. As a leading implementer of US Government Internet freedom programming, and with a global network of trainers and participants, Internews is well-placed to develop a framework to assess the impact of digital security training more effectively. This report contains a detailed framework complete with indicators, data collection tools and templates, and advice on how to use these monitoring and evaluation resources when conducting digital security training.

Working Toward a Digital Security Training Measurement Framework: Star Measurement Framework

The study informed the lead researchers' development of an initial digital security training measurement framework (which was further refined by Okthanks) to assess this kind of training more consistently and effectively. This first attempt at standardizing indicators, and monitoring and evaluation (M&E), across Internews is briefly outlined starting on **page 33**.

Building on the findings of this study and the indicators proposed by the lead researchers, Okthanks prepared the **Star Measurement Framework**. To enable trainers around the world to deploy the framework, Okthanks has built a set of user-friendly data gathering tools and resources. The Star Framework contains a process, worksheets, and reporting documents to guide a trainer or funder through a training evaluation. It provides advice on what information should be recorded, at which stage, and helps trainers collect, record, and report pertinent data. Star is divided into three components: before training, just after, and 3–6 months later.

Internews will continue working with Okthanks to test and refine this framework. Internews is currently piloting the Star Measurement Framework with select trainers and training participants, which includes training on the proposed indicators and data gathering tools, and financial support and mentorship. Feedback from this pilot will inform further refinements. Internews then plans to publicly share the revised framework, along with a brief summary of lessons learned from the test phase.

Methodology

In 2020, Internews commissioned user experience research and design organizations Okthanks and Superbloom to develop a research methodology to examine the experiences of digital security trainers. This early methodology[7] intended to deepen understanding of the trainers in Internews' international network, capturing emerging and established experiences, trends, and needs. Though it has not yet been deployed, that approach formed the basis of the research outlined in this report.

The lead researchers, Internews, Okthanks and Superbloom designed this research to better understand and document the challenges faced by digital security trainers, the resources available to them (and their use/perception of these), and the efficacy of their training.

The key research questions were:

- What challenges do digital security trainers face in measuring the efficacy of their training?
- What resources do digital security trainers need to measure the impact of their training, and can Internews provide those resources?

- What are the barriers preventing participants from adopting safer behaviors online after digital security training? What are some of the gaps between knowing better and doing better?

Prior to beginning the study, the lead researchers referenced the Kirkpatrick Model, a corporate and academic training evaluation framework, also known as the four levels of training evaluation.[8][9][10] The lead researchers drew heavily on this evaluation framework to devise a training impact model with four aspects: experience, learning, application, and impact (see **Figure 1**). The research team used this model to inform a theory of change and corresponding research methods to explore the best ways of understanding effectiveness in each of these four elements and form the basis of an initial digital security training measurement framework.

Figure 1. Training impact model used in this study

This research also drew heavily on the Okthanks and Superbloom Understanding the Frontline research methodology, notably in using online questionnaires incorporating its Priority Rating and some questions from its Diary Exchange. The focus group discussion (FGD) guides in this research study also incorporated questions from the Diary Exchange, and identified alternative opportunities to use a modified version of the Anxiety Games.

The research study took place in late 2021. Internews recruited five regional researchers, covering Latin America and the Caribbean (LAC), Sub-Saharan Africa (SSA), the Middle East and North Africa (MENA), Central and Eastern Europe (CEE), and Asia, to co-design and test the research tools and lead the deployment of the data collection methods within each of their target regions. Regional researchers were selected based on their contextual knowledge of the regions they covered, experience as digital security trainers, and vast networks of both training participants and fellow trainers. These five regions represent geographies with a high number of digital security trainings funded by Internews and

regions where Internews has an existing network of trainers and training participants. The respondents to this study are journalists, activists, academics, human rights defenders, civil society leaders, and digital security trainers.

The MENA researcher was unable to complete the study for personal reasons but contributed to the design and testing of the research tools. Internews was unable to recruit a replacement researcher for the MENA region due to timing constraints, but will seek input from trainers and participants in this region in the future.

Research Tools

The research tools (see **Appendix 1**) comprised:

- An online questionnaire for digital security trainers (in English and Spanish)
- An online questionnaire for training participants (in English and Spanish)
- An FGD guide for digital security trainers
- An FGD guide for training participants

After two online workshops to train the regional researchers on hosting effective FGDs and to refine the tools, each researcher was asked to carry out FGDs in their region, either online or in-person. The aim was to convene several groups of digital security trainers, and training participants, reaching at least 15 digital security trainers and 20 end users in each region. The online questionnaires were circulated by the regional researchers and Internews staff, to reach the widest possible range of respondents.

After the FGDs, regional researchers completed forms to summarize the responses they had received. The lead researchers collated and analyzed these forms and the online questionnaire results. The lead researchers also held two debriefing sessions online with regional researchers to ensure the former fully understood the findings, and to validate information on emerging themes, including regional similarities and differences.

Research Respondents and Implementation

The respondents to this study are journalists, activists, academics, human rights defenders, civil society leaders, and digital security trainers.

The regional researchers mostly recruited FGD members (and, to an extent, questionnaire respondents) from their own networks. This includes trainers they knew professionally,

and in some cases current colleagues. Many of the 'trainee' participants had received digital security training funded by Internews, and some had been trained by the regional researcher or were professional contacts of that researcher.

This research represents the views of 209 individuals. In total, 79 trainers and 43 training participants completed online questionnaires. And 47 trainers and 40 participants took part in more in-depth discussion, through focus groups, key informant interviews (KIIs) or written correspondence (see **Research Limitations and Challenges**).

Table 1 shows the region where each research participant was active. In total, the study included training participants from 12 countries and trainers from 28 countries. Two trainers reported that they also work in the US, and one in Spain, but these countries have not been counted in the table below.

Table 1. Regional distribution of research respondents

	Trainers			Participants		
Region	**Survey**	**FGD/KII**	**Total**	**Survey**	**FGD/KII**	**Total**
Asia	9	13	**22**	4	5	**9**
CEE	3	6	**9**	3	5	**8**
LAC	31	12	**43**	3	12	**15**
MENA*	0	0	**0**	0	0	**0**
SSA	35	16	**51**	33	18	**51**
Total	**79**	**47**	**126**	**43**	**40**	**83**

* The MENA regional researcher was unable to complete the study for personal reasons resulting in the lack of MENA respondents. Internews will seek input from trainers and participants in this region in the future.

The FGD/KII guides were administered by the regional researchers as written and agreed during the training workshop, minimizing the risk of significant bias. One FGD comprising a regional researcher's direct trainees was conducted by the lead researchers.

Research Limitations and Challenges

Coordinating the Research Team

Employing researchers who were embedded in their respective regions was a strength of this study, but such a widely disp≈ersed team brought coordination challenges. All regional researchers attended initial training together, but the post-research debrief had to be held in two separate groups to accommodate different time zones.

Recruiting Study Participants

As noted above, the MENA researcher was unable to complete the research.

The response to the online questionnaires was lower than expected. The regional researchers also found it difficult to recruit FGD participants, even for online groups. This was largely because people were busy with year-end work, and hampered by COVID-19 restrictions. The CEE researcher noted that a significant proportion of respondents had recently participated in other studies, possibly leading to fatigue.

The regional researchers tried to overcome this by offering one-to-one KIIs instead of FGDs, at times to suit interviewees, and by sending written questions to respondents so they could reply in their own time.

Research participants (particularly the survey respondents) were not evenly distributed among the target regions (see **Table 1**), but the findings remain useful for both regional and global overviews.

Participants' Attitudes to Training

The research respondents were self-selecting to an extent — by taking part in the research, they were arguably demonstrating a positive attitude towards the work they were doing/had done (in the case of trainers), or the training they had received (participants).

Therefore, no respondents had such a negative experience of working with the regional researchers that they were unwilling to respond to their request for input. So it is possible that this study is missing responses from people who have found digital security training less useful or beneficial.

Results

Engagement with Digital Security: Barriers and Enablers

Digital Security is a Low Priority for Training Participants

Only one FGD participant ('A') had a role that explicitly involved any kind of IT. This person's perspective was markedly different from those of other participants.

A works for a media organization in a role that encompasses digital security and general IT for the organization. It is A's responsibility to ensure that their colleagues, and the organization's data, remain safe online. A is therefore interested in learning as much as possible about digital safety. A also finds the topic interesting, so spends personal time reading about it and developing a network of people with similar interests.

In contrast, other participants (trainees) in the study saw digital security as a mystery and a chore. Both trainers and training participants indicated very low levels of interest in the topic, and the latter required persuasion to take part in training — viewing it as something they have to do to pursue their 'real' work.

Several participants described the 'whole world' of digital security as too overwhelming to understand. Trainers are acutely aware of this: one trainer from Eastern Europe described himself as 'a go-between, bridging the two worlds.' Another agreed that convincing someone to sign up for training feels like a significant achievement.

> *"I need somebody to speak my language when it comes to these things. I'm sure it's important, but I don't understand what people are talking about, so I tune out."*
>
> – Training Participant in Africa

In Latin America, people at coordinator or manager level tend to be more aware of the digital security risks faced by frontline workers and volunteers in their work and are open to training on the topic. But frontliners have less understanding of these risks and demonstrate less interest in digital security (requiring persuasion from coordinators/managers).

Enablers to Engagement with Digital Security

FGD participants in all regions said that what motivated them to attend digital safety training (often beginning their overall engagement with the concept) was a conversation with a friend or professional contact, who could present the value and benefits of the training in a straightforward and compelling way.

All regional researchers concluded that training participants are unlikely to act on digital security until they encounter a problem. And then, they only want to solve that problem rather than considering digital security more broadly. However, several trainers noted that learning about one digital security problem often prompts people's interest in training on additional issues.

Helping training participants to understand that digital security knowledge will help them to achieve their goals more safely and effectively is an aspect where trainers noted they could benefit from more support. Case studies which trainers can reference when recruiting training participants that demonstrate the practicality of secure behaviors is one example of this type of support.

Key factors that prompt people to access digital security training:

a. A clear understanding of the specific risks they face
b. A convincing argument that training and support can enable them to avoid, reduce or mitigate these risks (i.e., you can learn to fix this problem)
c. A recommendation from a friend or professional contact who has attended similar training

Accessing Training: Barriers and Enablers

Finding a Trainer

Training participants' experience of finding a digital security trainer varied widely by region. In SSA and most of LAC, there is a significant and growing community of digital security trainers with varying areas of expertise, who are relatively easy to identify and approach, though there may not be enough trainers to meet needs and they may be unevenly distributed.

> *"[This] is a country with many years of conflict where one would think they had enough time and resources to have a big community of trainers, but they don't… When you don't incentivize training of trainers, community building and there just aren't enough resources you get a country that desperately needs trainers and there's not enough people to meet the demand."*
>
> – Researcher in LAC

This is partly mitigated by the fact that people frequently access remote training with trainers in other countries in their region, but LAC participants are not satisfied with this. SSA participants also expressed a need for more digital security trainers in general, and also for trainers with specific areas of in-depth expertise.

In all regions, participants emphasized the importance of trust when searching for a trainer. This was particularly evident in Asia and CEE, where security concerns mean that trainers are harder to identify as they have to work more covertly. These security concerns may be related to operating in a country where there are legal restrictions on Internet freedom or if they are part of or serving a marginalized group (such as the LGBTQIA+ community) which is further at risk.

> *"Trust is a barrier. Not knowing where to look, or what to look for."*
>
> – Trainer in Asia

The majority of respondents said they used their personal networks to identify digital security trainers, which works well for people who are already part of the digital security or Internet freedom communities (or related groups). However, those who work alone or who are new to the digital space find it difficult to know who to trust, particularly if their work is very high risk.

Trainers and training participants all described a 'bubble' of digital security/Internet freedom actors — a community of individuals working in the sector who have built trusting relationships, so they feel safe to share challenges, resources and questions. These bubbles have no tangible presence and are closed to outsiders — only those on the inside have access to other community members.

> *"[Trainers] say that being in the bubble is a privilege, but it's hard to get into it. It's knowing the right person at the right time. Some trainers said it was because the nature of the bubble is very trust-*

> *based and it's hard to build trust. Most described their initial contact with the bubble as being luck-based."*
>
> – Researcher in LAC

In all regions, Internews is a key player in the digital security community, which is recognized as a provider of training, a facilitator of connections and perhaps an entry point to this bubble.

> *"When I recruited trainers for the research, there was a proportion who were connected to Internews, but…also… a bunch… who probably weren't. They were trainers who worked in [the] local context, and I knew them through the Internet freedom community."*
>
> – Researcher in Asia

> *"One trainer said that getting in contact with Internews was easier, more flexible [than connecting with others in the Internet freedom space]."*
>
> – Researcher in LAC

Characteristics of Trainers, and the Inclusiveness of Training

When asked about the relative importance of various characteristics in selecting a digital security trainer, participants broadly agreed that trainers' gender, age and ethnicity are a low priority, except for training on gender-sensitive subjects (such as gender-based violence, sexual and reproductive rights), where female participants would prefer (but struggle to find) female trainers. Anecdotal evidence suggests that digital security training is dominated by men, but there is no accurate data on the actual numbers of male and female trainers, due to their need to work covertly in many contexts. Participating trainers in CEE, most of whom identified as male, admitted to struggling to create gender-aware training, or to see its relevance.

> *"Donors require gender, disability, etc. sensitive training, but how can I adjust to different audiences if it's just about password training? Are donors putting unreasonable expectations on us? Or is it male trainers struggling to frame gender sensitive training or consider how audiences differ?"*
>
> – Researcher in CEE

Trainers' nationality was deemed unimportant in most regions, but respondents in Asia highlighted a need for more Chinese-speaking trainers.

Researchers noted a lack of trainers who identify as lesbian, gay, bi, trans, queer, questioning, intersex and/or asexual (LGBTQIA+), which may affect training uptake and require additional time to build trust in trainers. This is particularly important in locations where LGBTQIA+ people are stigmatized, and/or at risk if their identity is widely known.

> *"[Participants from the LGBTQIA+ community] feel safer and braver with a trainer who can relate to them, who comes from the same community."*
>
> – Researcher in SSA

Internews does not dictate the specific content or audience of digital security training funded through its programs, except in rare cases where trainers are asked to target a specific group (such as journalists), or reach a minimum number or percentage of marginalized people within the target group (such as women and people with disabilities).

> *"Often our focus is the trainers, with the theory… being, the more people we bring into the training community, the more they will work with their communities and spread digital awareness."*
>
> – Internews representative

This requires a balance between empowering trainers to meet the needs they have identified and challenging them to reach more marginalized communities. There is a risk that trainers largely reach 'people like us' and groups they are comfortable with unless they are pushed to seek out and include specific other demographics.

Expertise Required of Trainers

Training participants do not expect trainers to have specific expertise in the participant's field of work, but they do expect trainers to be able to apply digital security principles and practices to their work. However, across all regions, participants said it is important for trainers to understand the specific context in which they work, and have expertise in digital security, as it relates to their work and context. Participants are acutely aware that their knowledge is limited, and so look to trainers to diagnose issues, assess risks, develop materials and help them apply their learning.

> *"I want someone who can give me real-life experience."*
>
> – Training Participant in Asia

Trainers demonstrated an ability to adapt materials and resources according to very particular needs and contexts but the majority do so with no expectation of payment. However, trainers are realistic about their limitations.

> *"[Training participants] expect trainers to know everything, but trainers don't have this mindset. They expect to refer to other trainers/resources to fill gaps in their own knowledge."*
>
> – Researcher in CEE

This reinforces the importance of trainers' connections with other trainers and experts, and highlights the need for up-to-date and easily adaptable training materials and information. It was clear from the FGDs and KIIs that this continuous learning and problem-solving is a key part of trainers' work, and an aspect that they find enjoyable and motivating.

Who Pays for Training?

None of the trainers interviewed or surveyed reported directly charging participants for their training. Trainers' key motivators for working in this way are:

- The perceived benefits of connecting with participants with whom they might not otherwise connect; training can be an entry point for further collaboration
- Their own passion for, and commitment to, the issue
- The perception that participants would not be willing to pay for training

There is a risk that providing free training may reinforce any participants' perceptions that investing in digital security is not important, based on the idea that if something is free it has no value. However, trainers know their local contexts well, and their judgment is probably reliable on this.

Issues that Affect Training Content and Quality

Trainers felt that the quality of their work is affected by short-term funding, which limits the amount of time and resource they can dedicate to researching and developing new materials or approaches. Short-term funding also reduces the possibility of follow-up with trainees, to ensure that their learning is embedded and applied.

Ease of access to resources is heavily influenced by language. The vast majority of trainers find training resources online, and tailor them to their own language and context. LAC and SSA trainers in particular find that online resources tend to be created by, and target, people or organizations in the US or Europe.

> *"I have to read a lot of additional material and generate my own information. What's available is mainly tailored to North America or Europe. I can find interesting material, but it doesn't address risks… in Latin America. Also, resources and tools and platforms are in English. Some people in Latin America speak English but most speak Spanish, so it's a barrier to accessing content. There are community members who give time and resources to translating [training materials], but it's a lot of work and there aren't many people doing it."*
>
> – Trainer in LAC

Trainers make good use of the digital security community to share materials and information. In many cases they prefer this to accessing online information, as peer-sourced materials tend to be more up-to-date and contextually appropriate.

Applying Learning from Training: Barriers and Enablers

Almost all training participants (93 percent of training participant survey respondents) said they had applied part or all of the learning and tools they received from digital security training.

The most commonly reported enabler of implementing this learning was the **practical nature of the training**: 53 percent of training participant survey respondents mentioned the importance of having time to practice new skills during training sessions, and the ability to ask questions and apply the training to everyday work scenarios.

Nearly a third of training participant survey respondents reported that they had a new understanding of the importance of digital security after training, which motivated them to implement what they had learned.

> *"The idea of being safe online, ensuring my data is protected and preventing me from being a victim of online violence made it*

> *worthwhile."*
>
> – Survey respondent

For those who had not applied the skills and tools acquired in their digital security training, the key reasons were **Internet connectivity and access to devices**.

Internet connectivity was particularly reported as a challenge to putting digital security learning into practice in SSA and LAC, and to an extent in rural Asia. This is a huge frustration for participants and trainers, whose digital safety, and work, is limited by poor Internet access. It will be important for trainers in these locations to develop solutions and materials that require realistic bandwidth.

Access to digital devices was cited as a barrier to applying digital security skills and tools in CEE, SSA and LAC, but for different reasons. In Asia and SSA, for example, women's access to mobile devices is often controlled by men.

> *"Women come to training with devices but cannot change the security settings because they are secondary users. Most women use their husband's devices because they aren't allowed to own a smartphone – because if they had one, they would go online."*
>
> – Trainer in Zimbabwe

In LAC, participants and trainers reported that they often depend on the availability of government-financed devices, which can limit both the digital security measures they can implement, and the work they can do.

Survey respondents also highlighted the **cost of software** as a barrier to applying digital security practices, and other respondents mentioned the cost of digital devices.

> *"I have implemented everything that doesn't require software."*
>
> – Training Participant in LAC

Some 10 percent of training participant survey respondents (self-described human rights activists or international development workers) mentioned the importance of **support and buy-in from colleagues**, either as an enabler of, or a barrier to, applying digital security skills and tools acquired during training. This highlights the importance of ongoing digital security support at an organizational level, in addition to one-off training for individuals.

> *"I haven't started to use Mailvelope or other programs because nobody else in my organization uses them. So they wouldn't be useful.*
>
> – Survey respondent

For several participants, the issue was simply **the time required to adopt new habits** and behaviors.

> *"You are talking about human behavior. It is not realistic to change the behavior of one person, let alone a whole organization, overnight."*
>
> – FGD Participant in Asia

This is something trainers recognize, particularly if training covers something more complex than simply introducing a new password. In these cases, longer-term training and some ongoing support might be useful, such as follow-up calls from the trainer, or a WhatsApp group for sharing information or asking questions. Whatever form this support takes, it is crucial to recognize the additional work this creates for trainers, who should be adequately compensated.

Two of the training participants who reported in the survey that they had not applied the skills gained from digital security training, said they had not done so simply because they had forgotten. Two more gave lack of resources as the reason for not acting on their learning, and seven said they needed more training to do so.

Together, these participants represent 71 percent of the people whose training is not being put to use. These issues could potentially be resolved through follow ups from the trainer to provide encouragement, advice on accessible resources and further support as needed. Even peer support could resolve some of these issues, as other participants in the same regions said that they had been able to access software, for example.

Short-term Training Versus Ongoing Support

An unexpected but extremely significant finding is the emergence of two distinct approaches to training: short-term, one-off sessions or workshops, versus longer-term, ongoing support. The short-term model is most common in SSA and Asia, while ongoing support is beginning to dominate in CEE and LAC.

> *"Some of the trainers we approached for the focus group initially refused to participate, feeling that they shifted so much towards organizational security and away from short-term training engagements that they would no longer see themselves as 'trainers.'"*
>
> – Researcher in CEE

Trainers from SSA, Asia and also the other regions insisted that short-term training is still critical, and highly beneficial. Some training participants just need help with a specific issue, and trainers report that single-issue training frequently leads to demand for additional support. A large minority (41 percent) of surveyed training participants who had not implemented skills gained during their digital security training said they needed more input from the trainer. For example, one noted that the digital security context, threats and tools change so rapidly that one-off training quickly becomes obsolete. While this may be an exaggeration, the value of ongoing support should not be underestimated.

Already, 85 percent of trainers who completed the online survey indicated that they go beyond just providing training (see **Figure 2**). Most trainers recognized the principle that the trainer remains available to the participants for an extended period of time as the basis of their model.

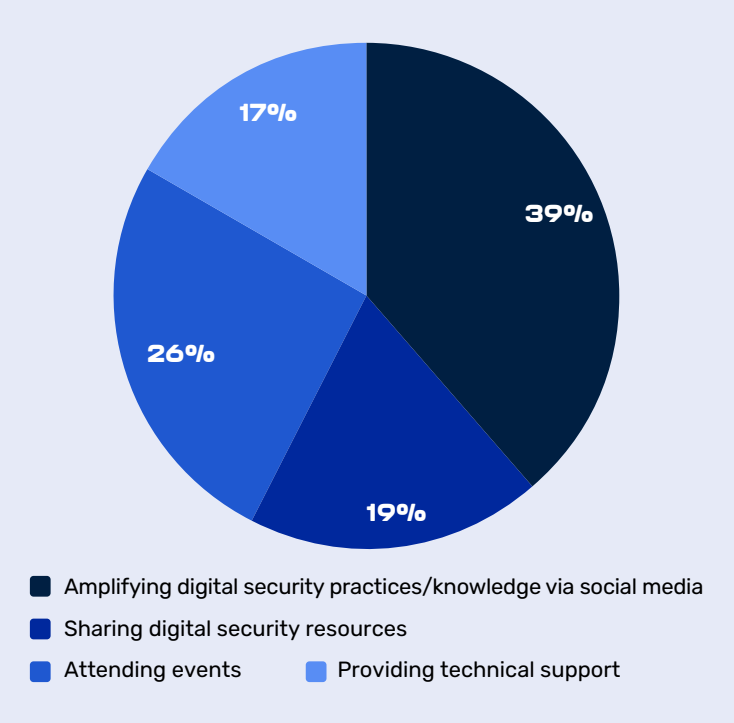


Figure 2. Additional support provided by digital security trainers

One trainer described a particularly involved model of ongoing support:

> *"I select an organization or network that needs support and choose focal points or a team… to work with. This team works with me from the start, from the risk assessment… They choose what kind of model they will use for the improvement of security. This group also chooses the topics for training. The group meets once a week for a learning session, or just to check in. During the [support] period, I also*

> *support [digital security] infrastructure and create policies."*
>
> – Trainer in Asia

Long-term relationships allow trainers to give more tailored input, and to support, encourage and motivate individuals and organizations as they implement their new digital security skills and knowledge. This ongoing involvement enables trainers to help participants react to issues as they arise, with many trainers reporting that they receive ad hoc requests for immediate help. Knowing the organizations well makes it easier for trainers to respond to these requests.

> *"Once a community finds a trainer, they tend to stick with them. This type of relationship isn't always just work-based, it turns into real-life friendships."*
>
> – Researcher in LAC

> *"This long-term, ongoing support is what's really needed. Digital security is not just one issue that can be solved by a training session. It's a whole mindset and approach."*
>
> – Trainer in CEE

Trainers who provide ongoing support also have a deeper understanding of the complex needs of the participant, gaining, as one trainer put it, *"the inside picture — what's really going on, not what people tell you in a needs assessment."* These trainers are also able to gain a broader view of participants' progress over time, and the impact of their training. If they deliver a two-day workshop and participants do not apply any of its learning, ongoing support trainers can clearly see this and provide additional support to facilitate application of digital security skills. This option is unavailable to trainers who have no contact with participants after delivering their training.

However, ongoing support also has disadvantages. For the trainer, the primary drawback is funding as ongoing support is rarely (if ever) paid for by participants. If an external funder does not fund ongoing support, trainers usually finance the work themselves. Some trainers have found ways to include ongoing support in funding applications.

The second drawback for trainers is the demand on their time. Providing what amounts to an on-demand helpline is fantastic for participants but can become unmanageable for trainers, particularly if they are supporting multiple participants at once.

Participants are aware of this, and a reluctance to 'impose' on a trainer without providing further payment is the most significant factor deterring participants in SSA and Asia from working long-term with their trainers.

> *"I haven't had an ongoing relationship with a trainer. It's unfair to expect the trainer to volunteer time and effort. There is no obligation on their side to be available."*
>
> – Training Participant in Asia

Some trainers providing ongoing support in LAC and CEE are beginning to establish boundaries with participants but find this difficult to negotiate, partly because they are so committed to the work.

Options for Measuring Impact

This study inspired a simple theory of change for digital security training: **if training participants learn how to improve their digital security, and if they implement that learning, then they will be less likely to experience the negative impacts of digital threats**.

The indicators included in this report cover all four aspects of training (experience, learning, application, and impact, see **Figure 1**), and each type of support provided, from awareness-raising, to training sessions and ongoing support (see **Measuring Impact** for initial proposed indicators arising from this study). Apart from general awareness-raising activities, the framework asks trainers to specify the training topic, to help gauge the level of increase in a specific knowledge area, or skills implementation.

The research findings reinforced the logic of a four-part training impact model, which reflects the participants' journey from awareness, through initial practice, to individual behavior change and then embedded habits. For organizations (rather than individuals), the final step would be systemic change at the organizational level.

Proposed Indicators to Measure Digital Security Training

This section outlines the lead researchers' proposed digital security training monitoring and evaluation (M&E) indicators based on the findings of this study. Not all indicators are applicable or feasible for every type of training. Training program implementers should determine the appropriate combination of indicators as part of their program design, ideally in collaboration with digital security trainers. Additional resources to support this process can be found as **Appendix 3** or in the accompanying **Star Measurement Framework**.

The lead researchers propose indicators in pages 34-38. The Star Measurement Framework, developed in coordination with Okthanks, is an example of how these indicators can be operationalized or deployed. Star goes beyond indicators, offering a full framework of worksheets and reporting documents designed to provide step-by-step guidance through a training evaluation. The indicators used in the Star Framework align with the proposed indicators in this report, with small edits to the language. Indicators help articulate what can be measured during a training, ultimately gathering data which will inform and improve future engagements with at-risk individuals and communities. Star resources are divided into three components:

- **Before Training:** The Training Profile captures critical information about the training, such as the structure, purpose, and specific topics which will be covered. This is the moment trainers or implementers should determine which indicators will be most relevant based on the goal and format of the training.
- **Just After Training:** Experience and learning indicators should be assessed just after the training takes place. Learning assessments can be administered to participants to determine how many people understood the training content and walk away with strategies to mitigate the risks covered in the training.
- **3-6 Months After Training:** The Star Framework merges application and impact into one category: change. Indicators related to change quantify how many people have applied learned strategies and have seen a direct impact as a result of their changed behavior.

The indicators suggested in this report are a result of the research and illustrate what can

be effectively monitored and evaluated. Star builds on that and offers tools and templates that can be used for data collection. As always with monitoring and evaluation, the aim is to gather evidence that demonstrates the efficacy of training and anyone using this framework should use indicators that are tailored to their situation.

Measuring Experience

Trainers and training participants both confirmed that measuring people's experience of digital security training is being managed well though, as noted in the Methodology, research participants are likely to be people who have had a positive experience of training.

Trainers appear to have adapted well to COVID-19 restrictions, combining in-person and remote training. Although trainers find it easier to gauge how well participants are following the training in person, they are tailoring their pace and delivery to accommodate different learning styles and levels of understanding. Of course, these reports come from trainers themselves, who are unlikely to report being bad at their work.

Proposed experience indicators measure process/activity only. External funders are likely to require the number of participants trained and/or the number of training hours provided, but otherwise these do not need to be compulsory.

Proposed indicators to measure experience are the number of:

1. Individuals reached through awareness-raising around digital security
2. Individuals provided with digital security support outside/in addition to formal training
3. Participants trained
4. Training hours provided[11]
5. Participants receiving ongoing support[12]
6. Ongoing support contacts
7. Participants receiving training with a focus on [any particular thematic focus]

Measuring Learning

Trainers reported a variety of methods for testing whether participants had understood the information shared during the training. These included pre- and post-training questionnaires, which is preferred by many donors but is an outdated method that is problematic.

A 1984 study for the informal education sector concluded that, before training, people are likely to under- or overestimate their skills.[13] This is true for digital security, which participants can find mysterious and overwhelming, yet through everyday use of digital tools they may have acquired knowledge in this field. The same study noted that, after training, people are likely to underestimate their understanding if they have found the training challenging, or if it has opened up new areas for them. This was consistently reported by the regional researchers, particularly those who work longer-term with participants.

> *"I used to do pre- and post-training surveys, but I stopped... since... it measures how much information [training participants] retain, not necessarily if they have learned anything and/or will apply it in their everyday lives. This is why I prefer [ongoing support] instead of evaluations because I can actually see it for myself. I feel like my own observations and judgment can be more useful than a post-training survey."*
>
> – Trainer in LAC

Participants' reported increases in knowledge, and pre- and post-training questionnaires, are flawed indicators and methods and therefore not recommended. However, they are so widely required by donors that they are included in the framework.

The proposed learning indicator using pre-/post-training tests and participant reports as evidence is:

1. The number of participants demonstrating an increase in knowledge or skills as a result of training

Trainers also described using in-training observation and continual assessment to see how well trainees are applying new skills or knowledge within the course setting. This includes asking questions to test understanding, presenting scenarios and asking trainees how they would proceed, or simply noticing who seems to be following, and who is lost. These assessment methods are much more effective, as:

- They enable the trainer to see immediately if material has not been understood by trainees, and to adapt accordingly — this opportunity is lost if testing takes place at the end of the course
- There is less pressure on trainees to 'perform' in a formal test
- They give the trainer the opportunity to identify needs for future training or support

In all types of training, relying on trainers' own reports is a potential limitation as it is not

possible to independently observe all training sessions, and trainers are not required to be trained, accredited or undergo performance reviews. If a trainer tells a funder that a group of participants acquired new knowledge, and the funder has no access to those participants, the trainer's word has to be accepted. This is not to question the integrity of trainers, many of whom are highly expert, but independent verification of participants' progress is not currently possible without commissioning external evaluations.

1. Proposed learning indicators using trainer reports are the number of:
2. Participants who understand the digital security threat as it relates to them and their work
3. Participants who are able to take measures to reduce/mitigate the threat
4. Participants/organizations with a strategy for ongoing action regarding digital security
5. Participants/organizations whose digital security strategy includes further training/coaching/support

Measuring Application

To an extent, the first two aspects of training (experience and learning) are within the control of the trainer. But after the training, responsibility for applying new skills and knowledge rests with participants. As Internews' primary relationship is with the trainer, and not all participants maintain relationships with their trainers, this makes ongoing monitoring difficult.

When trainers work alongside participants on a medium- to long-term basis, it is reasonable to ask trainers to track if/how trainees are using what they have learned from digital security training. These ongoing relationships also enable trainers to identify barriers to participants applying their learning.

For trainers who have more limited contact with participants, this follow-up is more challenging. As most participants receive training for free, it might be reasonable to insist on post-training follow-up as a condition of participation (such as trainees completing an online questionnaire or having a 30-minute call with the trainer three months after the training). This could be difficult to enforce but could be facilitated by the trainer diarizing follow-up action when arranging the training itself.

Proposed indicators for measuring application are the number of:

1. Participants who are implementing measures to reduce/mitigate the digital security threat[14]
2. Participants reporting having initiated a conversation around digital security with at least one colleague (within their organization or community of practice)
3. Participants reporting having initiated a conversation around digital security with at least one professional contact in a different organization or community of practice
4. Participants who have created information or training materials on digital security since their training
5. Participants who have delivered training to their colleagues using material created since their training or support
6. Individuals who have been trained by participants, using material created after receiving training or support

If post-training follow-up is possible, the first indicator is recommended as compulsory for any training program applying this framework. The remaining indicators in this list, relating to participants sharing knowledge with others, were suggested by research participants. Their rationale was that once you have understood something important yourself, you naturally share it with others — and this is an indicator of success. There is a risk that participants may share incomplete or inaccurate information but, on balance, any engagement in the issue of digital security could be regarded as positive.

Measuring Impact

For this aspect, the focus is understanding how/whether digital security training facilitated participants' work. The research indicates that participants can identify and attribute new behaviors or practices to attending digital security training. Examples given by trainers and participants include:

- People being able to do their planned work and feel secure about it, without repercussions/putting themselves at risk, because they could identify the right tools and techniques
- Organization digital security goals being matched with tangible steps
- No one in an organization has come under the threat that they identified at the beginning of the training even though they work in a risky context
- They have used their training to speak publicly about issues when there was intense scrutiny by the state

Proposed indicators for measuring impact are the number of:

1. Participants reporting a reduction in the negative impact of the specific issue targeted by digital security training or support
2. Participants attributing a reduction in the negative impact of the specific issue to actions they have taken as a result of the training or support

As with the application indicators, trainers can only report on impact if they have ongoing contact with participants, or at least the opportunity to conduct a follow-up survey or interview. When this is the case, both indicators should be compulsory.

The second indicator in this list allows participants to attribute positive change to the training they have received. The trainer (or whoever assesses the indicator) should ask for specific evidence for why the participant believes this. They might ask additional questions such as 'What other training or support have you had?', 'Where else have you discussed or heard about digital security?', or 'What else might have contributed to this change?'

Recommendations

Actionable recommendations arising from this research are organized into four categories.

Future Research and Testing: Additional Research Requirements

To include **voices from MENA** (see **Research Limitations and Challenges**), Internews should seek input from trainers and participants in the region. This could involve reusing the tools used for this study, or circulating and inviting comment on this report/the digital security training measurement framework.

To **maximize research participation**, any future research should be scheduled over a longer period (ideally not at the end of a calendar year). As well as using Internews-affiliated regional researchers, neutral third parties could recruit research participants, to minimize any personal bias relating to the researchers. Neutral researchers could also be contracted to host FGDs or KIIs.

To assess the quality and consistency of training, commission an independent observer to

assess training sessions (focusing specifically on the trainer's performance), or include assessing trainees' learning in future evaluations of funded projects.

Continue asking trainers and participants about the **enablers of, and barriers to, applying learning** gained from training, perhaps through a question in narrative reports or informal conversations, to direct support for trainers in the form of adaptations, materials or technical expertise to meet emerging needs.

The **framework to measure digital security training** developed through this research should be tested with people who have not been involved in this process — both Internews staff and trainers — and refined following their feedback.

Developing Materials: Equipping Trainers Appropriately

To improve the relevance and effectiveness of training, fund the development or refreshment of Global South-led, high-quality, accurate, up-to-date and accessible **digital security training materials** that can be re-used, adapted and shared widely.

To enable Internews to control the measurement standards and methods of its digital security training programs, support the development of a simple **curriculum for digital security training** by experienced trainers in the Global South, to include topics to cover and the basic, intermediate and advanced stages for each topic.

Identifying and Recruiting Trainers and Participants: Making Training more Inclusive

To **encourage participants to attend training**, work with trainers to create awareness-raising and recruitment materials for a range of audiences, including statistics and case studies relevant to participants' contexts and aspirations, in non-technical language. Alongside this, explore ways of using trainee cohorts to recruit new participants.

Particularly in locations where it has a physical presence, Internews could do more to **include individuals and groups who are outside the digital security community**,

either directly by Internews staff or indirectly through grantees.

To **identify which groups are currently under-served by digital security training** and direct resources to them, ask trainers to provide participant data that is disaggregated by gender, age, disability, etc.

Effective Funding: Appropriate Investment and Funding Advocacy

To help overcome commonly reported barriers to applying learning acquired in training, consider including funds to **broaden access to the Internet, digital devices and software** in grant and support packages. This might be complex to administer but could be considered for a pilot in specific locations. Consultations with local trainers could inform pilots and help to assess potential context-specific risks.

Funding for trainers should recognize the amount of time needed to prepare training, and to offer even basic follow-up support, not just the time involved in delivering training. In some cases, providing funding for 3–6 months would enable meaningful follow-up, strengthening both participant support and data gathering for reporting and learning. To support ongoing digital security support provided by trainers, consider increasing the quantity/proportion of funding available for this.

Additional Sources

Rasch, J (2022) How to measure your company's training effectiveness. Edyoucated blog. Available at: https://edyoucated.org/blog/company-training-evaluation-measures

Jay, S (nd) Training Effectiveness: A practical guide. Academy to Innovate HR blog. Available at: https://www.aihr.com/blog/measuring-training-effectiveness/#:~:text=Measuring%20training%20effectiveness%20can%20be,assess%20the%20data%20you%20collect

Lewis, J et al (1994) Performance Measurement and Evaluation Open University MBA Degree Programme, Block 3 Unit 9. Available at: https://openlearncreatelive-s3bucket.s3.eu-west-2.amazonaws.com/f1/1c/f11cc7ee89fbddd1c15ec34b52aa4e124eb87dc4?response-content-disposition=inline%3B%20filename%3D%22b889_1_courseguide.pdf%22&response-content-type=application%2Fpdf&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAUGDHWV25PIQSIQVT%2F20230605%2Feu-west-2%2Fs3%2Faws4_request&X-Amz-Date=20230605T164205Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21595&X-Amz-Signature=3a3186d36f75edf4c79c1a27109ba174a7b259d283ea41206cc7f6c448592d77

Pulley, ML (1994) Navigating the evaluation rapids. Training & Development, 48(9), 19+

Unboxed Staff (2021) How to measure training effectiveness using training evaluation metrics. Unboxed Training & Technology. Available at: https://unboxedtechnology.com/blog/what-are-some-metrics-for-evaluating-training-and-development/

Appendices

Appendix 1: Research Tools

Regional researchers translated these tools into their local languages. The parts highlighted in blue are places for each researcher to insert local information.

Focus Group Discussion Guide: Training Participants

Thank you very much for attending this group. I have asked you to be here because I am interested to know your views and experience related to digital security training. I am part of an international research team, and we will be using what you say to guide our research on how digital security trainers measure the effectiveness of their training. When we report on the work, we will not mention you by name [add other risk management info here].

You should express yourselves freely, and you have the right to not speak or answer any questions you feel uncomfortable with. You are also free to leave the group at any time.

Everyone is encouraged to speak, and I will give priority to people who have not spoken. One person should talk at a time. It is okay to disagree, but please respect each other's views. There are no right or wrong answers.

My name is [ ] and I will be leading the discussion. The discussion will also be recorded so that I can review your responses at a later date.

Needs Assessment and Training Design

What kind of work do you do? (eg, journalist, activist on LGBTQ+ rights/democracy)

Thinking about digital rights, freedom of expression, online safety, etc: what training have you had in this area in the last year?

How do you identify your training needs?

How do you find and choose a trainer? How easy is it for you to find a trainer? How easy is it for you to access training?

How do you pay for training? (eg, out of your organization's core budget, or through specific funds)

What training would be useful for you?

Support

Apart from training, I'm interested in what other kinds of support might be useful for you. (Show list on screen — do not read the list aloud) Of these, which is most important for you? Why? Which is least important? Why?

Is anything missing from this list?

- Connections and sharing with other activists/journalists near you
- Connections and sharing with activists/journalists in other countries or regions
- Ongoing support and relationships with trainers
- Training that's relevant for the communities you work with
- Working effectively in a closed or risky context
- Working effectively in a highly gender-biased context
- Anything else?

For [the most important issue for you], how easy is it to find support on this? What are some of the barriers to getting this support?

Training Delivery

Let's talk about what makes great training. Here are some examples to start with. (Show list on screen — don't read it aloud) Of these, which is most important for you? Why? Which is least important? Why?

Is anything missing from this list?

- Characteristics of the trainer (age, gender, nationality, etc)
- Trainer is an expert in the subject
- Trainer is an expert in my area of work
- In-depth coverage of theoretical aspects
- Focus on practical examples during the training

- I can implement what I've learned immediately
- Anything else

(If there's time, discuss each one)

Vignette (30 Minutes)

(Work through one of the vignettes)

Afterwards: What were the most challenging parts of this?

How easy would you find it to prove the effectiveness of your work, and how would you do it?

How do you think trainers could prove the effectiveness of their training?

Vignette A

Ana needs advice

- Ana advocates for greater transparency from her government, in a very closed context
- Most of her work involves raising awareness amongst young people
- Since the outbreak of COVID-19, Ana has to work mostly online
- 65 percent of the young people she worked with before the pandemic say that they are afraid of engaging online, because of government restrictions
- Ana has previously received some funding from the Rights Now Foundation
- The Foundation is now offering Ana additional funding to extend her social media campaigning and reach more young people BUT only if she and her team can find ways to work safely online
- Ana has only ever used Instagram for personal use, and sometimes Twitter for work

1. The need

- How can Ana identify what she and her team need?
- How can Ana define or quantify the problem she needs help with? (eg number of young people who don't want to engage, number of other campaigners who have received police warnings, new legislation she's unaware of)

- Where can she find this information?

2. Ana's Trainer/s

- How can Ana find the right trainer/s?
- How can Ana make sure the trainer really understands her needs?
- Apart from training, what else might Ana need?
- How might Ana make this happen?

3. The Impact of the Training

- How will Ana know if she and her team have understood the training?
- How will Ana know if she and her team are putting their learning into practice? What might they be doing differently from before?
- How might Ana's work be more effective because of the training?
- What should Ana say to the foundation?

Vignette B

Andre needs advice

- Andre is a human rights journalist who works with a wide variety of sources, for example:
  - » a border guard will soon be stationed at an outpost with no signal, except on government devices
  - » an activist who is working in a relatively safe environment but is very concerned about safety, and only wants to use Signal on burner phones
  - » an opposition politician who knows absolutely nothing about digital security
- Andre has been offered some funding from the Rights Now Foundation to write a series of articles about human rights
- Andre is concerned about how he can protect the people he interviews
- He knows he has a duty of care towards his sources, and needs to advise them on how to stay safe as they communicate with him but he doesn't have any experience or knowledge in this area

1. The need

- What are the key risks Andre and his interviewees are facing? (eg surveillance, interception of messages)
- Where can he find this information?
- How can Andre identify what he needs?

2. Andre's trainer/s

- How can Andre find the right trainer/s?
- How can Andre make sure the trainer really understands his needs?
- Apart from training, what else might Andre need?
- How might Andre make this happen?

3. The impact of the training

- How will Andre know if he has understood the training?
- What might Andre do differently as a result of the training?
- How might Andre's work be more effective because of the training?
- What should he say to the foundation?

Impact of training

Thinking about the digital rights, freedom of expression and/or online safety training you have had in the last year: have you implemented all of the skills and tools you learned?

If yes, what motivated you to do this? What enabled you to do it? (eg did you get additional follow-up support?)

If no/partly, what prevented you? (prompt, eg geographical, political, financial, time)

Do you intend to implement the skills and tools from the training? What support do you need to do this?

Can you give any examples of training that has had a real impact on your work? What did you change as a result of the training? What was the result?

Closing

Is there anything else you think we should have discussed, or any other questions?

Thank you for your time, I hope that you have found this interesting and useful. If you have any further question or thoughts, please feel free to contact me by email.

Focus Group Discussion Guide: Trainers

Thank you very much for attending this group. I have asked you to be here because I am interested to know your views and experience related to digital security training. I am part of an international research team, and we will be using what you say to guide our research on how digital security trainers measure the effectiveness of their training. When we report on the work, we will not mention you by name [add other risk management info here].

You should express yourselves freely, and you have the right to not speak or answer any questions you feel uncomfortable with. You are also free to leave the group at any time.

Everyone is encouraged to speak, and I will give priority to people who have not spoken. One person should talk at a time. It is OK to disagree, but please respect each other's views. There are no right or wrong answers.

My name is [ ] and I will be leading the discussion. The discussion will also be recorded so that I can review your responses at a later date.

Needs Assessment and Training Design

What frontliners do you support? (eg, journalists/activists — what issues do they address?)

How do you support them? (prompt, eg, training, demos, blogs, resources)

How do you assess your trainees' needs? Why do you do it this way?

How do you choose a topic for training?

How do you design your training — where do you get the content from?

What data do you collect about your trainees, and when? How do you store it? How do you use it?

Planning your Training

What objectives do your training generally have? (eg, themes, topics, fields)

What resources do you need for your work?

What, if any, additional support/resources would be helpful (eg, staffing, educational, materials, finances)?

How easy or difficult is it to find this support? What are some of the barriers? (eg, cost, time, risk, don't know where to look)

What resources or programs have supported you to improve as a trainer? How did you access these resources?

Training Delivery

How do people let you know if you're going too fast/too slowly, if they're too hot or cold, etc?

How can you tell if people are understanding the training while it's happening? How do you know if people are engaged, and 'getting it'?

Do you use any tools or techniques to check?

What feedback do you collect following the training? What do you do with it? Why do you do it this way?

What impact has COVID-19 had on your work? How has it changed how you work?

Vignette (30 Minutes)

Work through one of the vignettes (included above, see **Vignette A**, **Vignette B**).

Afterwards: What were the most challenging parts of this?

How easy would you find it to prove the effectiveness of your work, and how would you do it?

What would help you to do this?

Post-training Follow-up

Do you stay in touch with trainees after training? Why? How? For how long?

How do you know if people are putting your training into practice?

Can you give examples of how your trainees have succeeded in their work as a result of

your training?

Closing

Is there anything else you think we should have discussed, or any other questions?

Thank you for your time, I hope that you have found this interesting and useful. If you have any further question or thoughts, please feel free to email me.

Appendix 2: Surveys

Online Survey: Training Participants

Question	Options
Welcome! How do you identify?	Male/Female/Other (please state)
Which country do you normally work in?	
Do you work mostly in urban or rural areas?	Urban/rural
How would you describe yourself?	Human rights activist/digital rights activist/journalist/media worker/civil society leader/other
Have you received any training on digital security, staying safe online, freedom of expression, internet freedom, etc, in the past year?	Yes/no
If yes, have you implemented the tools and practices you learned from the training?	Yes/partly/no
If yes, what enabled you to do this?	
If partly/no, what prevented you from doing this?	
If partly/no, what support do you need to implement the training?	
What kind of training and/or support would be useful to you?	
How do you prefer to receive training?	Online/in person/combination of online and in person
Has COVID-19 changed your view on this? Please explain	
Priority rating	
How important to you are each of these? 1 = not important — 5 = very important	Connections and sharing with Activists/journalists in other countries or regions Connections and sharing with other activists/journalists near you Improving the usability and accessibility of tools/platforms
How much support do you currently receive in each of these areas? 1 = none — 5 = enough	Ongoing support and relationships with trainers Training that's relevant for the communities I work with Working effectively in a closed or risky context Working effectively in a highly gender-biased context
What are some of the barriers to getting [the training] you need?	Cost/time/risk/don't know where to look/other (please state)

What do you think makes for great training? Please rank in order of impact 1 = the most impactful, 8 = the least impactful	Trainer is an expert in the subject Trainer is an expert in my area of work Trainer provides additional materials/ resources for me to read outside the training In-depth coverage of theoretical aspects Focus on practical examples during the training I can implement what I've learned immediately Value for money Other (please state)
Thank you for taking part in this survey. If you have any questions about this study, please contact [researcher's name]	

Online Survey: Trainers

Question	Options
Welcome! How do you identify?	Male/Female/Other (please state)
Which country do you normally work in?	
Do you work mostly in urban or rural areas?	Urban/rural
How many years have you been training people?	
What themes or topics do you train people on most often?	
Who do you train and/or support?	Human rights activists/digital rights activists/ journalists/community groups/other
How do you support them and/or their work?	Training/attending demonstrations/amplifying social media/sharing resources/other
Priority rating (i)	
How important is this? 1 = not important — 5 = very important	Financial support (eg, support for logistics, staff, resource development) Connections and sharing with other trainers near you Connections and sharing with trainers in other countries or regions Emotional and mental wellbeing of you and your team Opportunities to develop new skills Attending international or regional conferences Working effectively in a closed or risky context
How much support do you currently receive in this area? ([priority area]) 1 = none — 5 = enough	

What would be a typical group size for your training?	1–9 10–15 16—20 20+
How do you recruit trainees for your training?	They come to me for bespoke training/I advertise through social media
On average, how much do you charge per person, per day, for your training? (Please include the currency)	
In a 'normal' year, how many times do you give training related to digital rights/internet freedom?	1–5 6–10 11–20 21–30 30+
Since COVID-19 began, how many times do you give training related to digital rights/internet freedom?	1–5 6–10 11–20 21–30 30+
What do you use for training? (to arrange it, deliver it and follow up)	Email/mobile phone (call)/mobile phone (text)/WhatsApp or other messaging service/Other (please state)
What do you use to measure what people have learned through your training?	Pre- and post-training tests/my own judgment/tests or quizzes during the training/other (please state)
How important is this? 1 = not important — 5 = very important	Building relationships with communities I'm not a part of Developing/accessing training materials that are relevant for the communities I work with Improving the usability and accessibility of [training] tools/platforms Maintaining/continuing relationships with trainees after training Measuring behavior change (eg, adoption of secure practices and tools) Working effectively in a highly gender-biased context
How much support do you currently receive in this area? ([priority area]) 1 = none — 5 = enough	
What additional support would help you?	
What are some of the barriers to getting what you need?	Cost/time/risk/don't know where to look/other (please state)

Appendix 3:

Sample Post-training Questions for Trainers

To support trainers in gauging the progress their training participants have made, this appendix includes a set of sample questions. Digital security trainers can use these as the basis for online, in-person or phone surveys or interviews, enabling consistent measurement of each indicator.

A limitation of these questions is that there is no standard curriculum for digital security. To evaluate and partly standardize digital security training, it would be beneficial to have a simple framework of progression for each subject area.

For example, for mitigating phishing attacks targeting a human rights organization, we might see:

Stage 1	**awareness:** participants (employees) understand the definition, meaning and potential impact of 'phishing'
Stage 2	**basic skills:** participants can identify phishing emails by [clue 1, clue 2, clue 3]
Stage 3	**implementation:** participants know how to safely deal with phishing emails by doing [action 1, action 2, action 3]
Stage 4	**systemic adoption:** participants detect and report phishing attempts to their organization, and the organization is able to raise awareness of phishing strategies internally and for other at-risk organizations

These questions follow the same categories as the framework (learning, application, impact). In each category, there are:

- Sample questions for which trainers would fill in the gaps, according to the subject of their training
- Sample questions with gaps completed related to the phishing example listed above
- Suggestions for observation activities

Learning – did participants understand their training, and can they recall it?

Questions *(blue = specific examples relating to phishing, as above)*

1. Why is it important to [do what the training covered]?

1. Why is it important to verify the sender of an email?

2. How can you identify [the threat/problem you learned about]?

2. How can you spot a phishing email?

3. How should you [do the thing you learned about]?

3. How should you deal with a phishing email?

4. When/how often should you [do the thing you learned about]?

4. When/how often should you verify the sender of an email

Observation

1. (If meeting in person) Using your mobile/laptop, show me how you would [do the thing you have learned to do].

1. (If meeting in person) Show me how you would verify the sender of an email. Look at this email — imagine you have received it. What do you think about it? What would you do with it?

2. (If not meeting in person) Talk me through the steps you would take to [do the thing you learned to do].

2. (If not meeting in person) Talk me through how you would verify the sender of an email.

Application – are participants putting their learning into practice?

Questions *(blue = specific examples relating to phishing)*

1. When was the last time you [did what you learned to do]? How do you know when it's time to [do the thing you learned to do]? (If they respond, 'I have a reminder set on my phone/in my calendar,' ask to see it)

1. When was the last time you verified the sender of an email? How do you know when you need to verify the sender?

2. In the past week, have you [experienced the threat we discussed]? What did you do?

2. Have you received an email in the past week that you suspected was phishing? What did you do about it?

3. Have you changed anything on any of your devices, like installing new software?

3. Have you changed anything on any of your devices, like installing new software?

4. Have you had any challenges [implementing skills and tools covered in your training]? (Eg can't afford software/keep forgetting)

4. Have you had any challenges spotting or dealing with phishing emails?

5. Have you talked to anyone else about [the specific issue covered by training]? If so, who? What was their response?

5. Have you talked to anyone else about phishing? If so, who? What was their response?

6. Have you shown anyone else how to [do the thing you learned to do]? If so, who?

6. Have you shown anyone else how to identify and respond to phishing emails?

Observation

1. If you meet any of their colleagues or contacts, ask: has [participant] talked to you about [the thing they learned]? Have they shown you how to do it? Please show me! When should you do this? Why?

1. If you meet any of their colleagues or contacts, ask: has [participant] talked to you about phishing? Have they shown you how to spot phishing emails, and/or how to deal with them? Please show me/talk me through it! Why is this important?

Impact – are participants' lives better because they are putting this training into practice?

Questions *(blue = specific examples relating to phishing, as above)*

1. Have you experienced [specific threat or incident] in the past week/month?

1. Have you experienced a phishing attack in the last week/month?

2. Since the training, have you identified [the threat you were trained on] when you might have missed it before? Since the training, have you [done what you were supposed to do], rather than [doing what you're not supposed to do]?

2. Since the training, have you identified phishing emails when you might have missed them before? Since the training, have you deleted/reported phishing emails, rather than clicking on links in them or opening attachments?

OR IDEALLY for 1 and 2: In your pre-training survey, you mentioned that you [experienced this threat frequently] OR [frequently had problems because of this threat] OR [were anxious or frustrated because of this threat]. Has that reduced? If yes, why do you think this is?

OR IDEALLY for 1 and 2: In your pre-training survey, you mentioned that you were caught out by a phishing email at least once a week. Has that reduced? If yes, why do you think this is?

3. Apart from [doing what you were taught to do], are you doing anything else differently, which might contribute to a reduction in [the impact of the threat]? Has anything else changed in your workplace or home that might be a factor?

3. Apart from verifying the sender, are you doing anything else differently, which might contribute to a reduction in your exposure to phishing? Has anything else changed in your workplace or home that might be a factor?

4. If you aren't dealing with [the consequence of the threat] so frequently, how has your work or life changed? (eg, I don't waste time trying to retrieve data, I'm less anxious about online violence)

4. Now that you aren't negatively affected by phishing so frequently, how has your work or life changed? (eg, I don't waste time trying to retrieve data, I'm less anxious about online violence)

Endnotes

1 Bullen, G, Diehm, C, Robertson, T and Winfrey, C (2020) "Understanding Support for the Frontline: A methodology and toolkit for documenting the practices and experiences of digital security trainers"

2 Center for Strategic & International Studies (2023) "Significant Cyber Incidents" Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

3 Freedom House (2022) "Freedom on the Net: Countering an Authoritarian Overhaul of the Internet" Available at: https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet#tracking-the-global-decline

4 Bullen, G, Diehm, C, Robertson, T and Winfrey, C (2020) "Understanding Support for the Frontline: A methodology and toolkit for documenting the practices and experiences of digital security trainers"

5 For brevity, 'FGD' is also used here as shorthand for these other forms of in-depth, qualitative responses.

6 Center for Strategic & International Studies (2023) "Significant Cyber Incidents" Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

7 Bullen, G, Diehm, C, Robertson, T and Winfrey, C (2020) "Understanding Support for the Frontline: A methodology and toolkit for documenting the practices and experiences of digital security trainers"

8 Kirkpatrick, D (1954) "Evaluating Human Relations Programs for Industrial Foremen and Supervisors"

9 The Standard for Leveraging and Validating Talent Investments™. See: Kirkpatrick Partners (no date) What is the Kirkpatrick Model? Available at: https://www.kirkpatrickpartners.com/the-kirkpatrick-model/

10 Tamkin, P, Yarnall, J and Kerrin, M (2002). Kirkpatrick and Beyond: A review of models of training evaluation. Institute for Employment Studies, Brighton, UK

11 'Training hours' does not include preparation or follow-up. As identifying, translating and adapting materials constitutes a significant burden on trainers, this could be captured separately, particularly if there is interest in supporting the creation/development of Global South-led materials in more languages.

12 Tracking the number of hours provided through ongoing support would give an accurate picture of the impact of this model. Trainers are likely to underestimate the amount of support they give through ad hoc calls or emails, which could be captured using this indicator. The Diary Exchange activity may support this.

13 Bennett, DB (1984) "Evaluating Environmental Education in Schools: A practical guide for teachers." Available at: http://unesdoc.unesco.org/images/0006/000661/066120eo.pdf

14 The nature of digital security means that even when participants perfectly implement learning from training, they may remain vulnerable to the risks covered by training, or to new digital security risks. This does not represent a failure in training, which is why the first indicator is phrased this way. This section covers how far participants applied their training; its impact is covered in the next section.

Star Measurement Framework: Resources

How to Evaluate a Digital Security Training

Using Star

Handbook Version 2.0
Last Update: December 2022

Star contains a process, worksheets, and reporting documents to guide you through a training evaluation. It provides advice on what information should be recorded at which stage, and helps you collect, record and report pertinent data. Star is divided into three components: Before Training, Just After and 3-6 Months Later.

Star was made possible by a collaboration of researchers, frontline trainers and Internews.

Internews OKTHANKS okthanks.com

About Star

Evaluations help you learn. They generate knowledge to inform future support. Knowledge that helps sponsors and trainers move the needle forward on meaningful change for individuals and communities.

SAVVY

Makes learning and change measurable

Star criteria help articulate what you can measure about a training. They are formulated around a simple theory of change: If participants learn how to improve their digital security, and if they implement that learning, then they will be less likely to experience the negative impacts of digital threats.

FLEXIBLE

Works with any curriculum

Star works with any digital security curriculum. It uses **threats** as the common denominator in trainings. Evaluations are then based on how well individuals understand and can mitigate the threats covered within a topic area.

ADAPTABLE

Made for you

Star intends to be adaptable to your needs and priorities. If the full package doesn't work, use the parts that do. Feedback is welcomed by the team.

Star Handbook Contents

To Guide the Evaluation Process

- A Star How To (This doc)
- B Learning Assessment Worksheet
- C Change Assessment Worksheet

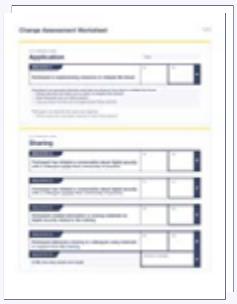
For Reporting and Reflection

- D Training Profile
- E Spreadsheet (3 Tabs)

Resources are available as separate documents.

A

B



C

D

E

Before Training

Plan

- [ ] ❶ Fill out the Training Profile
- [ ] ❷ Choose Your Evaluation Criteria
  In the Spreadsheet

❶ Fill out the Training Profile

The **Training Profile** is your central place to document the training structure, purpose and qualitative data. For this task, you will write down basic information about the training and provide an outline of the curriculum. For basic information, include:

- Training Purpose, Engagement Type, Format, and if you will be following up in 3-6 months

As you move through the evaluation process, the **Training Profile** will be important when recording assessment data, gleaning insights and planning your next training.

👉 Duplicate the **Training Profile** document to use for yourself.

How to Outline Curriculum

Write out the **topics** you plan to train on during the training. Topics may include but are not limited to the following:

- Secure Communication
- Account Security
- Secure Browsing
- Social Media Security
- Secure File Storage
- Backing Up Data
- Mobile Phone Security
- Secure File Sharing & Collaboration
- Travel Security

For each topic, document the **threats** relevant to it. Then include the **strategies** you will introduce that address each threat.

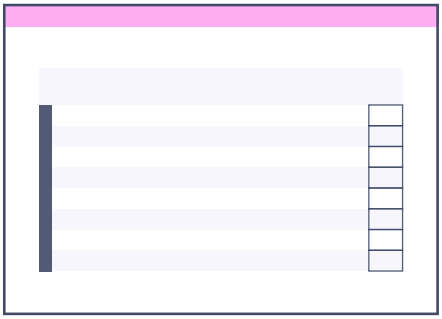
Topic	Threat 1	Strategies that address Threat 1
	Threat 2 (if applicable)	Strategies that address Threat 2
	Threat 3 (if applicable)	Strategies that address Threat 3

You may be training on more than one topic. If so, repeat the process of writing down your topic, accompanying threats and strategies for each. It's okay to include multiple threats and strategies for a single topic.

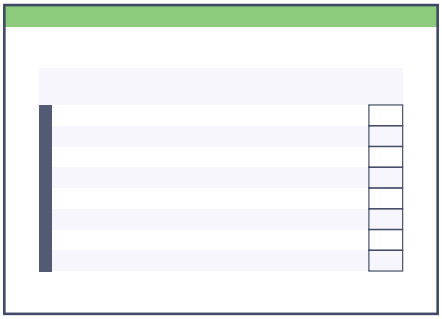
Before the Training

❷ Choose Your Evaluation Criteria

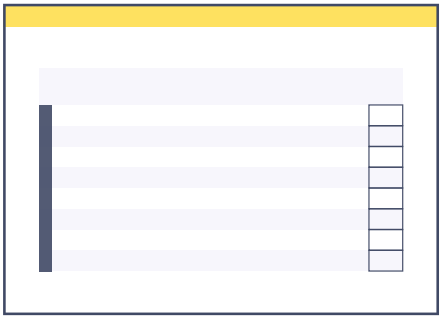
Review the evaluation criteria in the **Spreadsheet.** The Spreadsheet will be your central place to report measurements. The criteria and its descriptions are listed on 3 separate sheets: Experience, Learning, and Change. Each sheet has its own set of criteria relative to the objective of the category.



Experience criteria quantify how many people are trained directly or reached.



Learning criteria quantify how many people understand the training content and walk away with strategies to mitigate the risks addressed.



Change criteria quantify how many people have applied learned strategies and have seen a direct impact, along with how many people have shared what they've learned.

After reviewing, **choose the criteria that apply to the training**. Remember, the criteria help articulate what can be measured. What you choose will depend on what's important for you to learn. The examples below show how criteria may differ for 2 different trainings.

IF	THEN
If the purpose is to raise awareness in a one-time training	• Then, it may be important to know if participants understand threats and how to mitigate them. Use criteria L1-L5 and the open questions under training feedback. • The change assessment is not applicable.
If the purpose is to build skills, and the specific threats to participants are not fully known	• Then, it will be important to know if participants are able to apply the strategies from the training. Use criteria L2-L5 and the open questions under training feedback. • If you can talk to participants 3-6 month after the training or in a second workshop, use all criteria from the Change Assessment (C1-9). • As a part of this training, you may want to learn about the threats and concerns the participants face. Include additional open questions in the learning assessment to gain this knowledge. Have a plan to safely gather that information.

Just After

Evaluate learning & document participation

- ❶ **Conduct Learning Assessments**
  Using the Learning Assessment Worksheet
- ❷ **Record Assessment Results**
  In the Spreadsheet
- ❸ **Record Experience Data**
  In the Spreadsheet and Training Profile
- ❹ **Complete the Training Profile**
- ❺ **Share**

❶ Conduct Learning Assessments

At the end of a training or just after the training is the perfect time to find out if participants have walked away with new knowledge and strategies. The aim of the learning assessment is to measure participants' comprehension of the training content, and their ability to mitigate the threats associated with the topics covered.

Learning assessments can be conducted various ways.

- At the end of training: In-person survey, exit interview or pair & share.
- Scheduled time after training: Debrief interviews with training participants. They can be run by a trusted third party (preferred) or by the trainer themselves. A trusted third party decreases the likelihood of bias results.
- Asynchronously after training: Online survey

The **Learning Assessment Worksheet** provides questions to ask based on the criteria used. Refer to **page 7** for more information on how to use it.

⏰ **For the 3-6 month follow up, set a reminder on your calendar now!**
If you are following up with your training participants in 3-6 months you will have more assessment data to enter later. Don't worry, there is a separate sheet in the Spreadsheet to complete.

Just After

❷ Record Assessment Results

It's time to record your assessment data! Enter numbers from your **Learning Assessment Worksheet** on the Learning tab within the **Spreadsheet**.
Don't forget to record:

- How long has it been since the last training session?
- How many people actually completed the assessment?

❸ Record Experience Data

Begin by entering total participation numbers and hours on the Experience tab of the **Spreadsheet**. Then, document a demographic breakdown in the **Training Profile**. Include:

- Gender breakdown
- Country breakdown
- Subgroup breakdown

Document both your target numbers (these are who you hoped to train) and actual numbers (the number of people who actually showed up).

❹ Complete the Training Profile

The **Training Profile** is a great place to capture a training's overall impact and share those gems with others. It provides insight for you as a trainer to understand how you're doing, what people are learning, and where support is needed. Within the Narrative section include:

- Training feedback from the **Learning Asssessment**
- Quotes from participants (try to include 3)
- Aspects of how you conducted the training
- Things to focus on in the next training
- Support still needed for the community trained
- Date of next training (if applicable)

❺ Share

Great job.🍋 Now it's time to reflect and share what you've learned! The **Spreadsheet** and **Training Profile** are designed to be shared.

How to Use the Learning Assessment Worksheet

Assessment Worksheets can be used:

- When planning
- As an interview guide; or
- As an intermediary tool when translating responses into quantitative measurements

The **Learning Assessment Worksheet** contains open feedback questions, along with all of the criteria for learning. It's ordered in 4 sections: Training Feedback, Understanding the Threat, Threat Mitigation and Growth.

The questions under each criteria provide guidance on what to ask in a debrief interview. The goal is to understand if the participant satisfies the criteria; and gets a tally in the 'Yes' column. Some criteria have sub-criteria with supporting questions. These questions are a guide. You can decide which need correct answers to meet the criteria.

Translating into Measurements

If you're using the worksheet during an interview, tally answers along the way. In the end, you'll record the total number in the 'Yes' column in the Spreadsheet. You'll do this for each criteria.

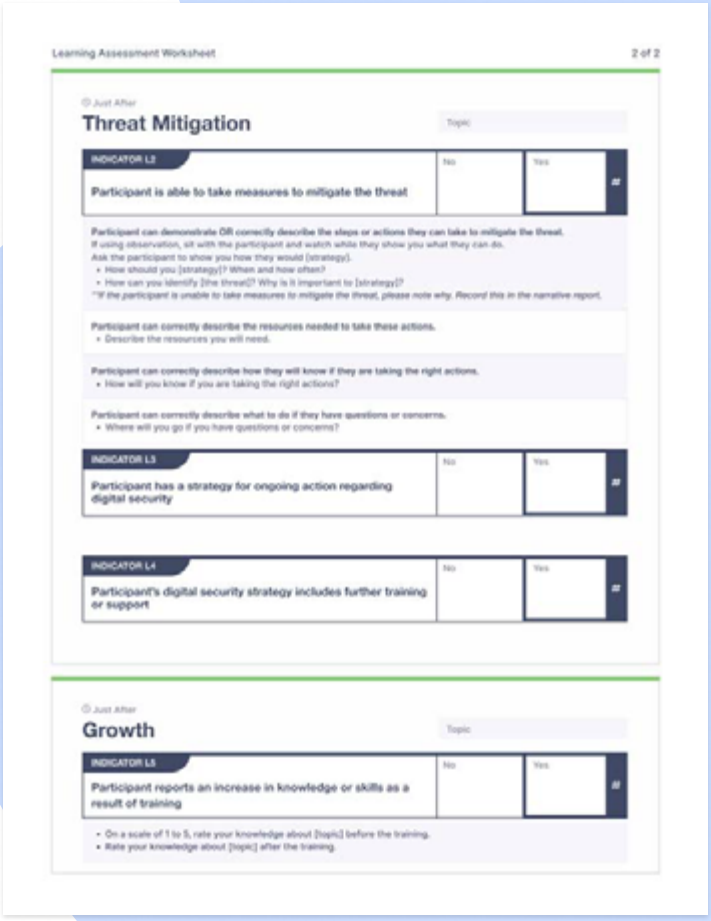
You will use one worksheet for each topic covered in the training. For example, if you have 3 topics, use 3 Learning Assessment Worksheets.

Recording Qualitative Feedback

The Training Feedback section is unique. It doesn't have a tally box for scoring. It's designed to help you gather qualitative information to inform future support and trainings. Record answers and/or synthesized findings from this section in the Training Profile.

WORKSHEET KEY

- **A** Example of guiding questions for the assessment
- **B** Scorecard
- **C** Signal to record in the **Spreadsheet**
- **D** Signal to record in the **Training Profile**



3-6 Months Later

Evaluate change

- ❶ Conduct Change Assessments
  Using the Change Assessment Worksheet
- ❷ Record Assessment Results
  In the Spreadsheet
- ❸ Update Experience Data
  In the Spreadsheet
- ❹ Update the Training Profile
- ❺ Share

In order to assess change, follow up with participants 3-6 months after the training. The aim of this evaluation is to understand if participants applied what they were taught, and what impact it has had. The **Change Assessment Worksheet** contains 4 sections: Application, Sharing, Impact and Growth.

Note: This step is not for everyone. If access to participants is impossible at this stage or your training purpose is simply to build awareness, this assessment does not apply to you.

❶ Conduct Change Assessments

Similar to the Learning Assessment Worksheet, you will need one **Change Assessment Worksheet** for each topic you trained on. Ideally, you will follow up with each participant from the training with a debrief conversation or survey. You will use the data recorded from this worksheet to inform the narrative report in the **Training Profile** and input findings into the **Spreadsheet**.

❷ Record Assessment Results

After you've completed following up with as many participants from your training as possible, enter the change assessment data into the **Spreadsheet** on the **Change** tab.

- Don't forget to capture:
  - How long has it been since the last training session?
  - How many people actually completed the assessment?

❸ Update Experience Data

If ongoing support has been provided outside of the training, quantify the number of people and interactions in the **Experience** tab of the **Spreadsheet**.

3-6 Months Later

❹ Update the Training Profile

Add notes and observations from the change assessment to the **Training Profile**. Include if people are applying what they've learned, and why or why not. It's important to understand if people are unable to mitigate threats. If this is the case, document why.

❺ Share

You're a Star! 🌟 You can share the **Spreadsheet** and **Training Profile**.

Acknowledgements

How it came to be

At the end of 2021, Internews commissioned research focused on the experiences of digital security trainers and the people they train—known here as participants. The research aimed to lay the foundation of an impact measurement framework that would better reflect the needs of the digital security training community. The lead researchers, Kate Long and Ellie Cole, partnered with regionally-based digital security experts. Together they conducted surveys, focus groups, and interviews to better understand the trainers' experience when assessing the impact of their work, and participants' experience receiving training and applying what they learn.

In 2022, the report, **Understanding the Global Digital Security Trainer Community**, was produced from the study. It outlines four assessment areas to use when evaluating a digital security training. These include: Experience, Learning, Application and Impact. Within these areas, **20** indicators in the impact measurement framework were defined.

During the end of 2022, Okthanks expanded the framework to include the assessment worksheets, the staged evaluation process and the training profile, offering guidance for collecting qualitative insight. The set of worksheets and accompanying resources are known as the Star Handbook.

Thank you

Star was made possible because of the regional research team, trainers and participants who took part in the 2021 research study. We particularly respect and recognize the dedication to excellence, inclusion and learning demonstrated by trainers who contributed to the study.

With gratitude, we'd like to specially thank; Ali Sibai, Cecilia Maundu, Chinmayi SK, Fabian Ziffzer and Łukasz Król, who co-designed and tested the research tools, and carried out research in challenging conditions. We would also like to thank Cecilia Maundu, Fabiola Maurice, Lukasz Krol, Happy Ayomirwoth Ongi, and Poncelet O. Ilelej, who willingly gave their time and expertise to review the Star Framework over the 2022 Holiday season.

A special thanks to our esteemed partners at Internews, who made the Star Framework a reality! Without their funding, valuable insight, dedication to prioritizing the needs of trainers and desire to positively impact communities around the globe with digital security, a measurement and evaluation tool would not be possible. Thank you, Amelia Ayoob, Ashley Fowler, Mia Vaccaro and Megan Guidrey.

Training Activities to Gather Feedback

Activities you can use during a training or right after to gather feedback. You can tailor activities to specifically address criteria you've chosen to collect data on.

Criteria Gathering Activities for During a Training

Pair & Share

After conducting a training or talking about topics (awareness-building) have participants pair up and work through a scenario together. Provide a scenario (relevant to the training you've just conducted). Pair people up in the room or in virtual groups. Show a slide, or write the scenario and provide prompts to help guide people through their discussion.

Example:

Training just completed on X topic (Secure Communication)—> Addressing X threat (account hacking)—> taught X strategy or capability to address the threat (2FA, strong passwords, password managers, locking devices, backing up content).

Scenario

Maria shares a device with her husband. She only has one email account which she accesses on the shared mobile device or at the library.

- **Prompt 1:** What can Maria do to keep her account safe?
- **Prompt 2:** write the steps Maria needs to take to implement one of the strategies you were just taught on
- **Prompt 3:** What other recommendations would you give to Maria about secure communications?
- **Prompt 4:** Do you think Maria is capable of implementing these strategies? Why or why not.
- **Prompt 5: L3** Are you capable of implementing any of the strategies discussed today? Which ones, why or why not?

- Prompt 6: **L4** Do you need more support or are you planning to attend more trainings on the subject within the next year?

*The Pair & Share activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L3**, **L4***

Dairy Exchange

This activity is meant to replace a traditional survey or post-training interview. It requires continued input from participants over a period of 3-6 months, but it can be simple and only take 10-20 min a week. Pair up participants (both from your training). Over the next 3-6 months they will be answering questions and keeping track of their behaviors and implementation of the knowledge that was learned and trained on in today's training. The pair will meet intermittently over the next couple months to discuss their answers and checkin on each other's progress. The pair will decide how frequently they will meet and what form of communication works best to communicate (signal chats, async whatsapp, video or phone calls, etc).

As a trainer, provide a list of things for the pair to discuss over the next couple months. Use questions which address criteria from the Experience, Change or Learning Assessment worksheets to gather necessary data. After 6 months (*as a trainer you can determine when to follow up*) the trainer will check back in with the pairs on their progress and gather feedback.

Sample Diary Exchange Questions

1. **L1**, **L2**, **C1** How have you been implementing the strategies learned during the training?
2. **L1**, **L2**, **C1** What has changed in your behavior because of the training? What are you doing or not doing differently?
3. **L2**, **L5**, **C7**, **C8** Have you experienced any of the threats discussed in the training? If yes, which ones? How did you respond? What actions did you take? On a scale of 1-5, rate the level of preparedness you felt when you experienced the threat.
4. **L5** On a scale of 1-5, how confident do you feel you know how to implement strategies (capabilities) taught in the training?
5. **L4**, **L3** Do you need more support or are you planning to attend more trainings on the subject within the next year?
6. **C2**, **C3** Have you shared any of your learnings with others since the training? If

yes, what have you shared?

7. **C2**, **C3**, **C4**, **C5** Have you conducted any trainings of your own or created any materials to share with others which came specifically from the training? **C6** IF you conducted a training, how many people attended?
8. **L4** Do you need more information or training on a topic? If yes, which topics?
9. **C1** How easy or difficult is it to get the resources you need? Rate on a scale 1-5, 1-being Easy, 5-being Difficult. Please Explain. What resources have you been using? **L4** What additional support would help you?
10. **L1**, **L2** What pain points or frustrations are you experiencing related to the topic, threat or strategies discussed during the training? Feel free to document any other concerns, frustrations or pain points (road blocks) you're experiencing that feel relevant.
11. **L4** Take a few minutes and think about how you envision the future. Now focus on digital and physical security. What does your future look like related to these topics? How is it different from today? What is needed to help your future become a reality?
12. **C1** Which resources, programs or strategies have helped you during these last couple months?
13. What advice would you give to a trainer as they design programs to support you or communities like yours?
14. Is there anything else you'd like to add or speak to?

*The Dairy Exchange activity can collect data points on Experience Criteria: **E1**, **E3**, **E4**, **E5** & Learning Criteria: **L1**, **L2**, **L3**, **L4**, **L5***

*During the 3-6 month follow up done by the trainer they can collect data points on Change Criteria: **C1**, **C2**, **C3**, **C4**, **C5**, **C6**, **C7**, **C8***

Waterfall

In the virtual world, where students and many adults are hesitant to turn their cameras on or unmute their microphone. Waterfall gives them a chance to participate in a safe low stake way. When everyone is contributing the focus is not on any one person. Waterfall can be used at the beginning of training, as a check for understanding during instruction, or as an exit debrief. It can also be a silly or personal question that fosters a sense of community.

Option 1

Ask a reflection question and have participants write their answers in a chat or shared riseup pad at the same time!

Participants answer in the chat, but do not click send

Trainer says or projects an image "3-2-1 Waterfall!"

Participants all press **send** together for a cascade of answers!

Option 2

Pair up participants and distribute prompts (or write them somewhere) have them talk through a scenario which addresses the topic & threat discussed during the training (or possible alternative scenarios) then together have them discuss a strategy or tactic to mitigate it or take proactive steps to prepare.

You can also have them answer the learning assessment questions from the Star Framework.

*The Waterfall activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L3**, **L4**, **L5***

Reflection/Debrief Activities for Just After A Training

Beach Ball

Blow up a beach ball and write a reflection question on each color slice. Gather participants into a circle and toss the ball around the circle 3 times. On the third catch the participant who caught the ball, reads the question closest to their right thumb and answers it. Each participant gets one option to 'phone a friend.' If they don't want to answer they can toss it to someone to answer. Repeat the process until everyone has answered.

Reflection question ideas:

- **L1** What is one thing you learned from today's training?
- **L2** What steps will you take to implement what you learned today?
- **L2** Share a strategy from the training.

Addresses L5, L2, L1

*The Beach Ball activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L5***

Spider Web

Gather participants into a circle, using a strand of yarn (or something similar) toss the yarn around the circle. When a participant catches the ball of yarn, they must answer a 'reflection' question before tossing it to the next person. At the end of the game (once everyone has answered), pull the strands tight (have people walk backwards until the web is taught). Then pluck a strand and see how many in the 'web' felt the vibrations. A fun way to display we are all in this together. Digital security connects us all! Strengthening one individual's digital security can affect others.

Reflection question ideas:

- **L1** What is one thing you learned from today's training?
- **L2** What steps will you take to implement what you learned today?
- **L2** Share a strategy from the training.

*The Spider Web activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L5***

Balloon Toss

Give a balloon to each participant (you could do this with paper, sticky notes, or something else fun). Each participant writes a threat related to the training topic. Or, have people write a question they want answered about the topic. Have them blow up their balloon. Get in a circle and have everyone toss their balloons into the air. Keep the balloons afloat for 10 counts or play some music and when you stop the music everyone must be holding a balloon. Then go around the circle and have everyone answer the question or provide a strategy to mitigate the threat that relates to the question on the balloon they are holding. You could have them write their answer on the balloon as well. Then share aloud or find a way of giving people back their balloons.

*The Balloon Toss activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L5**?*

Lineup

Option 1

First explain how the activity works: "This line represents how you feel about the statements

I'm going to make. This end of the line (point to one end) is the "strongly disagree" end of the line and this end of the line (point to the other end) is the "strongly agree" end of the line. The middle of the line is "neutral." I will read a statement and you need to place yourself on the line depending how much you agree or disagree with the statement"

Give the group a practice statement such as "I really like chocolate ice cream." Ask them to place themselves on the line based on how much they agree or disagree with this statement.

Then move into asking reflection questions. It is a quick way to count numbers, but it doesn't provide in-depth answers. If you want more information, call on a few people along the line and have them explain their decision.

Option 2

Have everyone stand in a straight line. Ask a series of reflection questions and if their answer is 'yes' have them step forward.

Sample Questions:

1. I enjoyed today's training
2. **L1**, **L5** I learned something in today's training?
3. **L2** I know a strategy to implement from today's training?
4. I will share with others something I learned from today's training?
5. I would participate in a training of this nature again?
6. I'd like to learn more about the topic or strategy we learned about today?

*The LineUp activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L5***

Quick Reactions

Use emojis or thumbs up👍, down 👎and shrug 👍🤷to answer reflection questions.

See Okthanks' Exploratorium activity, *Quick Reactions* for more instructions https://okthanks.com/quick-reactions.

*The Quick Reactions activity can collect data points on Experience Criteria: **E1** & Learning Criteria: **L1**, **L2**, **L5***

Express Yourself

Before & After

At the beginning of your training, or when you introduce a new topic within the training, have participants choose a number (from 1-10, 1-I know nothing-10, I'm an expert) regarding the level of knowledge they feel they have about the topic. Let them write the number on the front of a piece of paper. Title it 'before', then turn the paper over until the end of the training.

Then at the very end of the training, have them rate themselves again, this time on the back of the paper (title the back, 'after'). Then let them turn it over and see if there's a change.

You can ask follow up questions, debrief the training, or discuss why people chose the number they chose.

Example:

On a sticky note or a printed paper that has a scale on both sides (they could also draw a scale) write or make an ♀ on the number you choose. Turn the paper over. Trainer, continues training. You can gather more in-depth answers by asking participants to share about their rating.

On a scale of 1-10 (one being I know nothing and 10 being I'm an expert), rate your personal knowledge about [x topic].

The Before & After activity can collect data points on Experience Criteria: ***E1*** *& Learning Criteria:* ***L5***

Graffiti

Ask participants to draw a picture or use words to describe what the topic is and what they know about it. Then after the training, draw/ or describe a strategy or something they learned from the training. You can gather more in-depth answers by asking participants to share about their drawing.

Option 2

Using a shared piece of paper ask participants to describe with words, or drawings what the topic is you are about to discuss or train on.

After the training, ask participants to describe what they learned and what was talked

about using words or drawings on the same piece of paper. They could adapt what they drew or wrote at the beginning of the training. You can gather more in-depth answers by asking participants to share about their drawing.

The Graffiti activity can collect data points on Experience Criteria: ***E1*** *& Learning Criteria:* ***L5***

Group Debrief

At the end of a training session gather participants into a seated circle. Thank them for participating and let them know for the next 10–20 min you'll collectively provide feedback on the experience and the training. Let them know it is important to be honest and if they ever feel uncomfortable providing feedback verbally they can write down their feedback and give it to you afterwards. This is a time to listen and observe, take notes and capture feedback. It is also an opportunity to dig deeper into people's responses to truly understand what they learned, what was helpful and what to do differently. Try to get everyone involved.

Sample Questions to discuss:

- **L1**, **L2**, **L3** Go around the room and ask participants to verbalize one thing they learned from today's training.
- **L2** Ask for volunteers to share what strategies (capabilities) they learned today.
- **L2** Ask for a show of hands of how many people think they will actually implement one or more of the strategies (capabilities) learned from today's training.
- **L1**, **L2**, **L3** Share something helpful from today's training.
- **L3** What, if anything, will you do differently at home because of the experiences you had while participating in this training?
- **Training Profile** If we did this training again, what could we do to make it better?
- **L3** Are you capable of implementing any of the strategies discussed today? Which ones, why or why not?
- **L4** Do you need more support or are you planning to attend more trainings on the subject within the next year?
- **L5** Go around the circle and ask participants to self-assess what they knew prior to the training and then after the training.
- Is there anything from today's training that you would share with a friend, family or colleague? If yes, what would you share?

Training Profile

This is your primary place to record qualitative and contextual information about your training. This document is meant to be duplicated and used as your working document. Refer to the '**Star How To**' for complete instructions.

Before a Training

Basic Information

Training Purpose: What does the training intend to do?

- Raise Awareness
- Teach Skills
- Assist with Adoption of Tools and Practices

Engagement Type

- Single
- Series
- Ongoing

Format of Training

- Virtual
- In-Person
- Hybrid

Will you be following up in 3-6 Months?

- Yes or No

Curriculum Outline

To outline the training curriculum, you will document the following items *(as shown in Table A below)*. For full instructions, refer to the '**Star How To**.'

- Topics you plan to cover
- Threats associated with each topic
- Strategies that address the threats

Topic	Threat 1	Strategies that address Threat 1
	Threat 2 *(if applicable)*	Strategies that address Threat 2
	Threat 3 *(if applicable)*	Strategies that address Threat 3

Table A. Curriculum Outline

If the training covers multiple topics, copy the table above. Use one table per topic.

Just After a Training

Where was the training located?

Who was trained?

- *Please note if there is a particular vulnerable community or subgroup that was included in the focus of the training.*

Total number of people trained

- Include the target (who you hoped to train) versus the actual (who actually showed up)
  - Gender breakdown
  - Country breakdown
  - Subgroup breakdown

Narrative

Training feedback from the **Learning Assessment**

- Things to improve
- Other topics participants would like to learn
- Most useful things learned by participants

Quotes (try to include 3)

Aspects of how you conducted the training

- Which methods or activities did you implement?
- What would you repeat?
- What would you do differently?

Topics, strategies, tools, facilitation techniques, etc. to focus on in the next training

Support still needed for the community trained

Date of next training

3-6 Months Later

Narrative Report

- If people are unable to mitigate threats, please explain why.

STAR SPREADSHEET

Experience

Complete after training. Update through support phases.

Indicator	Definition	Number	
		Actual	Expected
Participants trained	Number of participants who have attended the training course		
Training hours provided	Number of contact training hours with participants (not including preparation or follow-up)		
People provided with digital security support outside of or in addition to formal training	Number of individuals reached by activities that are lighter-touch or more general than formal training, and constitute part of an ongoing relationship with a participant (individual or organization). This could include ad hoc phone calls, troubleshooting, workshops, etc.		
People receiving ongoing support	Number of individuals directly supported through at least one phone call, email exchange, or similar means after the initial training		
Ongoing support interactions	Number of times you have provided support, through phone, email, in-person or other means. Count each time you have been in contact with a participant, even if you have had several conversations about the same issue.		

STAR SPREADSHEET

Learning

Participants Assessed: *Time Since Training:*

Complete just after training.

	Indicator	Definition	Number
L1	**Understanding the Threat:** Participant understands the threat as it relates to them and their work	Number of participants who can correctly describe: ▪ the nature of the threat ▪ potential sources of the threat ▪ the practical implications of the threat for their personal safety and security ▪ the practical implications of the threat for their organisation's safety and security (if relevant) ▪ the practical implications of the threat for their work	
L2	**Threat Mitigation:** Participant is able to take measures to mitigate the threat	Number of participants who can correctly demonstrate or describe: ▪ the steps or actions they can take to mitigate the threat ▪ the resources needed to take these actions ▪ how they will know if they are taking the right actions ▪ what to do if they have questions or concerns	
L3	**Threat Mitigation:** Participant has a strategy for ongoing action regarding digital security	Number of participants who have a written plan that sets out future actions for improving digital security (beyond immediate actions from this training)	
L4	**Threat Mitigation:** Participant's digital security strategy includes further training, coaching, or support	Number of participants with a written plan that recognizes the need for further training and support	
L5	**Growth:** Participant demonstrates an increase in knowledge or skills as a result of training	Number of participants who, directly after the training or support, report improved knowledge or skills in the topics covered	

STAR SPREADSHEET

Change

Participants Assessed: *Time Since Training:*

Complete 3-6 months after training.

	Indicator	Definition	Number
C1	**Application**: Participant is implementing measures to mitigate the threat	Number of participants who can describe or demonstrate steps or actions they are taking or have taken that would be reasonably expected to mitigate the threat: ▪ precisely what they are doing or have done, and how ▪ how frequently they are taking the action (if relevant) ▪ the resources involved	
C2	**Sharing**: Participant has initiated conversation about digital security with a colleague inside their community of practice	Number of participants reporting conversation about a specific digital security topic with at least one person within their organization or community of practice	
C3	**Sharing**: Participant has initiated conversation about digital security with a colleague outside their community of practice	Number of participants reporting conversation about digital security at least one professional contact in a different organization or community of practice	
C4	**Sharing**: Participant has initiated conversation about digital security with a colleague outside their community of practice	Number of participants who have adapted the information provided in training to share as information or training within their organization. Only count the participant if the information they have created is accurate and appropriate.	
C5	**Sharing**: Participant delivered training to their colleagues using materials or support from the training	Number of participants who have used skills and knowledge acquired during training to train their colleagues or other professional contacts.	

STAR SPREADSHEET

Change (continued)

	Indicator	Definition	Number
C6	**Sharing**: Individuals (who did not attend the training) who have been trained by participants, using material created following training or support	Number of individuals who have received training from participants who were trained under this project.	
C7	**Impact**: Participant reports a reduction in the negative impact of the specific issue targeted by training or support	Number of participants who record and report change in their personal and/or organizational experience.	
C8	**Impact**: Participant attributes the reduction in the negative impact of the specific issue to actions they have taken as a result of training or support	Number of participants who record and report change in their experience, and have evidence to suggest that this change is a result of specific actions they have taken.	
C9	**Growth**: Participant reports an increase in their ability to mitigate threats as a result of the training	Number of participants who report an increase in their ability to mitigate threats after the training or support	

Learning Assessment Worksheet

Just After

Training Feedback

OPEN QUESTIONS

Record answers to questions below in the Training Profile.

- What would you improve?
- Which other topics would you like to learn more about?
- What was the most useful thing you learned.

Just After

Understanding the Threat

Topic

CRITERIA L1	No	Yes	#
Participant understands the threat as it relates to them and their work			

Participant can correctly describe the threat.
- Why is [topic] important?
- Which problems can be avoided?
- Describe the threat. Who do you need to protect against?

Participant can correctly describe potential sources of the threat.
- Which individuals or organizations might want to attack you in this way?
- How might the threat arise through negligence or accident?
- How might the threat occur in different locations and on different devices?

Participant can correctly describe practical implications on their personal safety and security.
- What might happen to you if this threat occurred?
- How might family or friends be affected?
- How could this digital threat affect my physical safety?
- Do you have non-work-related devices and accounts that would be affected?

Participant can correctly describe practical implications on their organization's safety and security. (If applicable)
- How might other colleagues be affected?
- If one person is affected, would there be an impact on the organization as a whole?
- What could be the impact on the personal safety for everyone in the organization?

Participant can correctly describe practical implications for their work.
- How would this threat impact the effectiveness of your work?
- What would be the impact of this threat on your finances, reputation, and ability to operate?
- Could the people you serve be directly or indirectly harmed?

Just After

Threat Mitigation

Topic

CRITERIA L2	No	Yes	#
Participant is able to take measures to mitigate the threat			

Participant can demonstrate OR correctly describe the steps or actions they can take to mitigate the threat.
If using observation, sit with the participant and watch while they show you what they can do.
Ask the participant to show you how they would [strategy].
- How should you [strategy]? When and how often?
- How can you identify [the threat]? Why is it important to [strategy]?

***If the participant is unable to take measures to mitigate the threat, please note why. Record this in the narrative report.*

Participant can correctly describe the resources needed to take these actions.
- Describe the resources you will need.

Participant can correctly describe how they will know if they are taking the right actions.
- How will you know if you are taking the right actions?

Participant can correctly describe what to do if they have questions or concerns.
- Where will you go if you have questions or concerns?

CRITERIA L3	No	Yes	#
Participant has a strategy for ongoing action regarding digital security			

- Please share how you will stay up to date on digital security moving forward.

CRITERIA L4	No	Yes	#
Participant's digital security strategy includes further training or support			

- Do you have plans for additional training, coaching, or support?

Just After

Growth

Topic

CRITERIA L5	No	Yes	#
Participant reports an increase in knowledge or skills as a result of training			

- On a scale of 1 to 5, rate your knowledge about [topic] before the training.
- Rate your knowledge about [topic] after the training.

Change Assessment Worksheet

3-6 Months Later

Application

Topic

CRITERIA C1	No	Yes	
Participant is implementing measures to mitigate the threat			#

Participant can precisely describe what they are doing or have done to mitigate the threat.
- Please describe the steps you've taken to mitigate [the threat]?
- How frequently are you taking action?
- Can you show me how you've implemented these actions?

Participant can describe the resources required.
- Which resources have been required to take these actions?

3-6 Months Later

Sharing

CRITERIA C2	No	Yes	
Participant has initiated a conversation about digital security with a colleague inside their community of practice			#

CRITERIA C3	No	Yes	
Participant has initiated a conversation about digital security with a colleague outside their community of practice			#

CRITERIA C4	No	Yes	
Participant created information or training materials on digital security related to the training			#

CRITERIA C5	No	Yes	
Participant delivered a training to colleagues using materials or support from the training			#

CRITERIA C6	Number of people	
If YES, how many people were taught.		#

Change Assessment Worksheet 2 of 2

3-6 Months Later

Impact

Topic

CRITERIA C7	No	Yes	#
Participant reports a reduction in the negative impact of the specific issue targeted by training or support			

- Regarding the [threat/issue addressed in the training], how has your personal experience changed?
- How has the experience of the organization changed?

CRITERIA C8	No	Yes	#
Participant attributes the reduction to the actions they have taken due to the training or support			

- Do you have any evidence to suggest that this change is a result of the specific actions taken due to the training?

3-6 Months Later

Growth

Topic

CRITERIA C9	No	Yes	#
Participant reports an increase in their ability to mitigate threats as a result of the training			

- On a scale of 1 to 5, rate your ability to mitigate the [threat] before the training.
- Rate your ability to mitigate the [threat] after the training.

25
X25

Internews

internews.org
info@internews.org
@internews
facebook.com/internews