# IMPROVING DIGITAL LITERACY AND SECURITY TRAINING IN CAMBODIA





MAY 2022

Maura Joul, Annie Kemmerer,
Baker Lu, Billy Taki

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Innovations for Social Accountability in Cambodia (ISAC) is a five-year, United States Agency for International Development (USAID) funded project working to improve public service delivery in Cambodia through the application of social accountability tools. ISAC works through seven grantee partners to improve social accountability across eight Cambodian municipalities.

DAI oversees ISAC Objective 3, which aims to increase the utilization of new or existing enabling technologies for citizens to hold local governments accountable for delivery of public services. To implement ISAC Objective 3, DAI will provide technical support to Digital Information and Innovation Fund (DIIF) grantees to design and roll out new digital tools/technology solutions; design and deliver trainings about digital tools and technology; and promote digital security among implementation partners (IPs). To support this objective, graduate students from Johns Hopkins University School of Advanced International Studies (SAIS) conducted a landscape assessment on digital literacy and security education and training initiatives in Cambodia. The landscape assessment maps and assesses the quality of these initiatives and provides recommendations that will inform ISAC investments into digital literacy and digital security programming for civil society organizations (CSOs) in later years of the program.

After identifying existing digital literacy and security initiatives in Cambodia, research focused on addressing the following key questions:

- Who are the key partners and target audiences of various initiatives?
- How do training providers reach their target audiences?
- What are commonly used training approaches?
- How do implementers measure quality and/or impact of programming?
- What makes specific initiatives particularly successful?

The report highlights trends and commonalities among existing digital literacy and security initiatives in Cambodia, best practices for training initiatives, and gaps in CSO digital capacity. Based on these findings, the report concludes with actionable recommendations for specific stakeholders, including USAID and other funders, ISAC and other training providers.

## KEY FINDINGS AND RECOMMENDATIONS FOR USAID AND OTHER FUNDERS:

### Findings:

**Cambodia's rural provinces lack systemic digital programming and reliable internet connectivity.** Training providers that facilitate programs outside Phnom Penh report working on an *ad hoc* basis, limited by minimal broadband infrastructure, low computer ownership rates, and low levels of local digital literacy. Despite this lagging digital capacity, however, it is still possible to conduct trainings in rural provinces as mobile internet users can access social media, mobile applications, and a wide range of business and financial services.

**Key stakeholders – including the government, training providers, and content creators – do not adequately disseminate or exchange information on important issues, content, and players in the ecosystem.** Interviewees mentioned barriers to gathering information on digital training initiatives in Cambodia due to low volume of publicly available resources and a lack of information sharing mechanisms among key stakeholders. As the digital training ecosystem develops, there is a need for funders to design communications strategies to help spread public information and promote industry-wide knowledge transfer about digital literacy and digital security trainings.

**Many CSOs lack a permanent and trusted IT staff member.** CSOs in Cambodia rely heavily on certain digital tools to conduct their work; however, many lack in-house IT staff. Having a knowledgeable, trusted internal IT team (or staff member) is a crucial part of ensuring good digital hygiene at the organizational level. While part-time or shared resources can help CSOs meet certain IT needs, not having at least one fully dedicated IT staff member leaves CSOs more vulnerable to cyberattacks.

**CSOs lack internal trainings about digital literacy and security and do not have access to external trainings tailored to their needs.** Some interviewed CSOs provide minimal internal digital security training for their staff, either due to a lack of resources (some have no permanent IT staff), not prioritizing digital security, and/or a dangerous assumption that staff are already well-versed in IT and cybersecurity issues. CSOs require training on digital security topics, as well as the judgment and critical thinking to bridge the gap between simply understanding the basics of digital security topics and actually exhibiting safe behaviors in practice.

## Recommendations:

**Increase programmatic investment outside Phnom Penh.** Increased investment in widespread digital training can address gaps in local capacity, resulting in a larger digitally literate population capable of using computers and operating safely online. Some options for reaching CSOs in rural provinces include systematizing *ad hoc* training programs, traveling conferences, and/or public information campaigns.

**Support knowledge sharing among key stakeholders.** Greater information and knowledge sharing about digital security and digital literacy initiatives among relevant stakeholders can help improve programming, increase transparency, and potentially bring more funds into Cambodia's digital development space. To this end, funders could foster clear communication around which data and reports are private and which can be shared among CSOs and other individuals and organizations working on digital literacy and security.

**Allocate more funding for IT staff.** Many Cambodian CSOs have a clear, urgent need for upgraded internal IT capacity, specifically for a full-time IT staff person who can build trust by maintaining an ongoing relationship with staff members. Funders could require that *all* organizations applying for funding have demonstrated access to IT expertise, which could lead to improved digital hygiene practices across Cambodia's CSO community.

**Fund and support internal and external IT training programs for CSOs.** CSOs can further lower their risk of falling victim to digital threats by ensuring that all staff are adequately trained on important digital literacy and security topics. While IT personnel can implement these trainings, access to external trainings is necessary for CSOs that lack these internal resources.

# KEY FINDINGS AND RECOMMENDATIONS FOR ISAC AND OTHER TRAINING PROVIDERS:

## Findings:

**Low pre-existing digital literacy and critical thinking limit the effective transfer of digital literacy and security skills and knowledge.** Interviewees frequently cited the limitations of pre-existing digital literacy and critical thinking skills as a barrier to

effectively teaching digital skills and hygiene. Given the high likelihood of continued videoconferencing in the training ecosystem, effective strategies to actively engage virtual trainees are increasingly important.

**Training providers experience difficulties assessing trainee progress and skill retention.** Follow-up to assess trainee progress and skill retention requires sufficient time and resources, but many training providers have small teams and limited funds. These organizations facilitate trainings with only one or two staff members while working within a fundraising ecosystem that often optimizes for training classroom size without similar incentives for promoting long-term follow-up. These issues highlight the importance of creating follow-up mechanisms that fit the training program's staff capacity and also proactively monitor participant progress and reinforce newly learned skills and behaviors.

**Training providers do not take advantage of pre-existing content.** Instead, the majority of organizations and content creators interviewed created their own curriculum, though some were mandated to use materials provided by an external funding organization (such as Meta). Those who did create their own content were expressly motivated by a pride in their work and typically built out content/curriculum based on their own professional experience conducting digital training programs. Beyond a lack of awareness of existing content, a couple of interviewees shared that other content creators were hesitant to use international materials due to translation and localization challenges.

**CSOs often do not understand the laws and regulations applicable to their work.** Several interviewees stated that CSOs and online users often lack an understanding of regulatory topics. Interviewees generally agreed that CSOs with an online presence require training on legal and regulatory topics related to their online activity.

## Recommendations:

**Promote hands-on and relevant learning over memorization.** Hands-on and scenario-based learning can elicit critical thinking, ensure that participants understand the "why" behind concepts being taught, and promote a broader understanding of how and when to apply these skills. Another effective teaching device is storytelling, where technical content is incorporated into a narrative to make it more tangible and emotionally engaging. In addition to storytelling, individual or group projects and assignments are also a popular and effective component of many interactive training programs. For organizations seeking to include a virtual component in their trainings, it is important to place a strong emphasis on ensuring that learners are able to ask questions and interact with content in a constructive way.

**Focus on training both hard skills and intuition.** Both digital literacy and digital security training programs typically include content on how to use relevant hardware and software, but it is important that digital security curricula are deliberately designed to foster judgment and critical thinking skills. Staff members must be trained to be constantly vigilant, understand *why* certain actions are preferable to others, and be aware of potential consequences.

**Use follow-up mechanisms to assess and reinforce behavior change.** With COVID-19 driving many trainings online, follow-up has become even more important for training providers to track participant learning outcomes and progress. Interviewees mentioned using mechanisms such as surveys, mentorship or coaching, a volunteer help desk and social media groups to track participant progress.

**Carefully adapt international content for local audiences and invest in producing high quality Khmer language training materials.** To reduce unnecessary duplication of content, training providers could lean on existing resources and channel their efforts toward carefully translating and contextualizing important concepts from international content. However, despite directly relevant international content, training materials still need to be localized for a Cambodian audience and reflect the specific digital literacy and security needs of the trainees.

**Include legal and regulatory content in digital security trainings.** Training CSOs on digital regulations relevant to their work helps protect them against potential legal vulnerabilities. The average CSO staff member does not need a fully comprehensive understanding of the legal environment - a general awareness about relevant regulations that apply directly to their work may be sufficient.

**Collaborate with key stakeholders to increase engagement, cross promote, and share best practices.** While employers can mandate training attendance, active participation and engagement are much more difficult to elicit. Thoughtfully selecting a like-minded partner can help increase the perceived value of new digital literacy and security training programs and amplify outreach efforts. In addition to providing engaging content, a partnership with a recognizable brand or well-known industry expert can lend credibility if learners are less familiar with the organization conducting the training.

# INTRODUCTION

Innovations for Social Accountability in Cambodia (ISAC) is a five-year, United States Agency for International Development (USAID) funded project working to improve public service delivery in Cambodia through the application of social accountability tools. ISAC works through seven grantee partners to improve social accountability across eight Cambodian municipalities.

DAI oversees ISAC Objective 3, which aims to increase the utilization of new or existing enabling technologies for citizens to hold local governments accountable for delivery of public services. To implement ISAC Objective 3, DAI will provide technical support to Digital Information and Innovation Fund (DIIF) grantees to design and roll out new digital tools/technology solutions; design and deliver trainings about digital tools and technology; and promote digital security among implementation partners (IPs). To support this objective, graduate students from Johns Hopkins University School of Advanced International Studies (SAIS) conducted a landscape assessment of existing digital literacy and security education and training initiatives in Cambodia.

The landscape assessment maps and assesses the quality of these initiatives and provides recommendations for ISAC investments into digital literacy and digital security programming for civil society organizations (CSOs) in later years of the program. The report also highlights trends and commonalities among existing digital literacy and security initiatives in Cambodia, best practices for training initiatives, and gaps in CSO capacity. Based on these findings, the report concludes with recommendations for specific stakeholders, including funders, ISAC and other training providers. These recommendations are particularly timely in light of more Cambodian CSOs coming online due to COVID-19; communications and programming shifting to virtual platforms; increased digital security issues in Cambodia; and political and legal changes at the local and national government levels.

The report will begin by outlining the research methodology used to conduct this landscape assessment, followed by information about relevant context and stakeholders. The report will then go over key findings before concluding with recommendations specific to individual stakeholder groups.

# DEFINING DIGITAL LITERACY, SECURITY, AND HYGIENE

*Digital literacy* is defined as "the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills."[1] In addition to operating a device, platform, or software, it includes the social and emotional ability to safely exist in online contexts.[2] Digital literacy is an umbrella term that includes information literacy, computer literacy, media literacy, communication literacy, and technology literacy.

*Digital security* is defined as "the collective term that describes the resources employed to protect your online identity, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices."[3] Digital security also includes a behavioral component and requires users to have the situational awareness to understand how and when to use certain tools in order to protect themselves online.

Both concepts are inextricably linked, and competence in one necessitates some level of proficiency in the other. Basic digital literacy, for example, requires knowledge and application of digital security practices. For clarity, the report will refer to digital literacy and digital security as separate terms, with digital hygiene referring to the combination of the two. *Digital hygiene* is defined as "the practices and steps that users of digital devices can take to maintain system health and improve their digital and online security."[4]

[1] ALA, "Digital Literacy."
[2] Eshet, "Digital Literacy: A Conceptual Framework for Survival Skills in the Digital era."
[3] Simplilearn, "What Is Digital Security: Overview, Types, and Applications Explained [Updated]."
[4] Plostins, Sour, and Oung, "Innovations for Social Accountability in Cambodia Initial Digital Assessment."

# RESEARCH METHODOLOGY

The SAIS team used a combination of desk research and stakeholder interviews to conduct a landscape assessment of digital literacy and security training programs across Cambodia. The team initially relied on academic papers; reports by government, nonprofit, and international organizations; and other online resources to map existing programs. However, this desk research revealed gaps in existing literature which emphasized the importance of conducting key informant interviews (KIIs) with individuals directly involved with digital literacy and security initiatives in Cambodia.

The SAIS team worked with DAI staff based in Washington, DC and Phnom Penh to compile a list of 25 relevant organizations and training initiatives and associated key informants for each. The team then developed a structured interview template that was used to conduct virtual interviews with these key informants. The template included questions across three key topic areas: the state of digital literacy and security in Cambodia; important digital literacy and security concepts and how to teach them; and details about each organization and training program. Appendix B includes the full list of interview questions.

The team initially conducted 14 virtual interviews with different informants including digital security consultants and content creators, training providers, local CSOs, international organizations, and industry experts. These interviews helped establish a list of emerging findings and themes that guided the team's fieldwork strategy. During the next research phase, the SAIS team traveled to Phnom Penh in January 2022 to conduct 16 in-person interviews using semi-structured questionnaires that emphasized the emerging findings and themes. Of these 16 in-person interviews, 12 were first-time interviews and four were follow-ups to earlier virtual interviews. In-person interviewees spoke more freely about their personal expertise and experience with digital literacy and security trainings in Cambodia, and these interviews allowed the team to validate preliminary findings and establish key recommendations.

# CONTEXT

## COUNTRY-LEVEL DIGITAL INFRASTRUCTURE

Overall, access to mobile services in Cambodia is strong. The proportion of mobile cellular subscriptions in Cambodia relative to its population is nearly 125%, a figure that exceeds both world and Asia Pacific regional averages.[5] More specifically, the Telecommunication Regulator of Cambodia reports that as of September 2021 Cambodia has over 17 million mobile internet subscribers (103% of the population).[6] While this figure is inflated because some subscribers may subscribe to multiple providers, another recent survey indicated that approximately 11.8 million Cambodians (~70% of the total population) have mobile internet access through personal or shared subscriptions.[7] In terms of mobile internet speeds, users of Cellcard, Smart Axiata and Metfone experienced 4G connection speeds or better for over 80% of the time that they accessed mobile internet.[8]

Although many Cambodians are able to access mobile internet, very few have access to fixed broadband internet on home computers at home. The fixed broadband penetration rate was only 1.1% as recently as 2019 and is projected to grow to only 3.0% by 2026.[9] In addition to inadequate fixed-line infrastructure, these low subscription figures are driven by low rates of computer ownership. In 2019, only 13.3% of Cambodian households owned a computer.

Large infrastructure gaps, especially in rural areas, have important implications for providing accessible training modalities such as virtual learning. A 2021 report found that only 70% of Cambodian youth in the less-developed Mountain Region have internet access as compared to 96% in Phnom Penh.[10] This disparity is also seen in smartphone ownership, with 93% of youth living in Phnom Penh owning a smartphone compared to only 66% of Mountain Region youth.[11]

[5] Beschorner, Neumann, and Martin, "Benefiting from the Digital Economy. Cambodia Policy Note."
[6] Telecommunication Regulator of Cambodia (TRC), "Phone Subscriptions."
[7] Fenwick, "Cambodia, February 2021, Mobile Network Experience."
[8] Ibid.
[9] Marshall, "Cambodia - Telecoms, Mobile and Broadband - Statistics and Analyses - Buddecomm."
[10] Sao, Ratan and Otdam, "Understanding How Young Cambodians Use Media and Information - Media Action."
[11] Ibid.

## DIGITAL LITERACY LEVELS IN CAMBODIA

Although Cambodia's internet penetration rate is high, many Cambodians do not possess important digital literacy skills; having access to and regularly using the internet does not automatically lead to the development of basic digital skills or hygiene. A UNDP study found that Cambodian youth score below global averages in ICT tests,[12] despite the fact that 87% of them use the internet frequently.[13] This skills deficiency also exists in professional organizations - a survey by the Konrad Adenauer Foundation found that surveyed Cambodian firms and organizations generally lacked digital skills in online information management, online collaboration and data analytics.[14] According to the International Telecommunication Union, less than 30% of Cambodians understand how to perform common professional digital tasks (such as using an Excel spreadsheet), and less than 1% of Cambodians are able to perform more advanced tasks such as finding, downloading and configuring software.[15] Cambodian CSOs have reported having difficulty finding digitally-skilled labor, as university IT graduates often cannot immediately perform the technical tasks required to work within these organizations.[16]

According to several interviewees, demographic characteristics (such as age) correlate with digital literacy levels and users' overall comfort using digital tools. Interviewees commonly referred to citizens that have grown up in the information age and are comfortable with a wide variety of online platforms and devices as "digital natives." They widely agreed that anyone 40 years old or younger in Phnom Penh could be considered a digital native, while in other municipalities, the age threshold may be as low as 30 years old due to less advanced digital infrastructure and less frequent use of digital tools in the education systems.

Finally, Cambodia's education system itself may be hindering digital skill development by emphasizing memorization and repetition over critical thinking skills and not fostering an environment in which students typically ask clarifying questions. Many interviewees stated that this pedagogical style has presented an important challenge to teaching safe cybersecurity practices in the country, as protecting oneself online requires the ability to

[12] United Nations Development Programme (UNDP), "Assessment of Digital Literacy for Employability and Entrepreneurship among Cambodian Youth: UNDP in Cambodia."
[13] Sao, Ratan and Otdam, "Understanding How Young Cambodians Use Media and Information - Media Action."
[14] Heng, Pheakdey, "Preparing Cambodia's Workforce for a Digital Economy."
[15] Banga & Willem te Velde, "Cambodia, Covid-19 and Inclusive Digital Transformation: A Seven-Point Plan."
[16] Plostins, Sour, and Oung, "Innovations for Social Accountability in Cambodia Initial Digital Assessment."

identify red flags, understand potential risks and their consequences, and use careful, timely judgments to make decisions.

## SOCIAL MEDIA USAGE IS GROWING, AND NEW USERS ARE UNEQUIPPED TO DEAL WITH THE RISKS

Cambodia's high levels of internet penetration have translated into widespread adoption of social media platforms. This adoption has accelerated since the beginning of the COVID-19 pandemic and associated lockdowns - the number of social media users in Cambodia increased by 2.3 million people (+24%) between 2020 and 2021, and by January 2021 nearly 70% of the population (12 million people) was on social media.[17] Facebook is one of the most popular social media platforms in Cambodia, with 11 million users in the country as well as 7 million Facebook Messenger accounts.[18] Telegram is also very popular, as many Cambodians use the platform to communicate with one another and receive important announcements from the government, though exact user statistics are unavailable. Both platforms are popular amongst Cambodian CSOs, who use them professionally for internal and external communications.

This widespread use of social media, and Facebook in particular, presents a unique digital security challenge to Cambodian CSOs and the general public, as many users fail to understand basic concepts about digital tools. In a recent survey where 47% of respondents in Cambodia reported having access to Facebook, only 38% reported having access to the internet,[19] which demonstrates a fundamental misunderstanding about how these platforms operate. Importantly, users also do not seem to understand what type of information is safe or appropriate to share online. The SAIS team spoke with multiple interviewees who mentioned witnessing friends or community members post personally identifiable information (PII) including cellphone numbers and banking information on Facebook and responding to messages from strangers online.

The increasing prevalence of online threats in Cambodia further exacerbates these vulnerabilities. During interviews, cybersecurity experts, CSO representatives and training providers reported a rise in the prevalence of cyber threats in the country, including phishing, viruses and hacking. The combination of the rise in online threats and relatively low levels of digital hygiene suggest a clear need to educate all Cambodians on how to better protect themselves online. CSOs in particular require more intensive training, as

[17] Kemp, "Digital in Cambodia: All the Statistics You Need in 2021 - DataReportal – Global Digital Insights."
[18] Heng, Pheakdey, "Preparing Cambodia's Workforce for a Digital Economy."
[19] Kem et al., "Cambodia's vibrant tech startup ecosystem in 2018"

they often work on sensitive topics with limited resources to purchase expensive digital security tools.

# KEY FINDINGS AND RECOMMENDATIONS

The following section of this report presents a list of key findings that demonstrate digital development obstacles faced by Cambodian CSOs, including gaps in overall digital capacity and specific limitations encountered by digital training providers. The first segment is targeted towards USAID and other funders focused on digital development and strengthening democracy and governance in Cambodia, while the second segment focuses on ISAC and other digital training providers (both organizations and individual content creators). Each set of findings is paired with a series of recommendations for actionable strategies that can improve the digital hygiene of Cambodian CSOs.

## USAID AND OTHER FUNDERS

The following findings are most relevant to funders, principally USAID and other donors, though some items might also be relevant for smaller funders, private foundations, implementing partners, or other organizations responsible for country-wide programmatic decision making. The findings are followed by a list of actionable recommendations, including examples of specific implementation strategies when applicable.

### Findings for USAID and Other Funders

#### *1. Cambodia's rural provinces lack systemic digital programming and reliable internet connectivity.*

Phnom Penh has vocational schools, digital education programs (in some schools), and an increasing number of digital jobs. Rural provinces, however, lack similar access to systematic digital training programs. With the exception of a few digital skills training programs in Battambang and Siem Reap, the vast majority of digital training programs are based in the capital. The government – through the Ministry of Education, Youth and Sport (MoEYS) – is working to improve digital skills training in schools in rural provinces and

make educational content readily available online,[20] but according to interviewees, there were no systematic programs in place targeting adults.

Training providers that facilitate programs outside Phnom Penh report working on an *ad hoc* basis, limited by minimal broadband infrastructure, low computer ownership rates, and low levels of local digital literacy. Rural villages often do not have any residents with sufficient digital skills or knowledge to run a training, and limited local digital infrastructure forces external training providers to adapt their programming. For example, trainings for citizen journalists outside of Phnom Penh often focus on how to write and send stories using smartphones, since computer access is typically unreliable or unavailable. Trainings and information campaigns around digital hygiene are especially important, as rural mobile internet users face similar risks of online threats to those in the capital but lack access to the same digital training programs.

Despite lagging digital capacity, however, it is still possible to conduct trainings in rural provinces, as mobile internet users can access social media, mobile applications, and a wide range of business and financial services. Some training providers explained that shifting programs online due to COVID-19 also expanded their geographic reach into the rural provinces, since accessing an online training is easier for many rural trainees than traveling to Phnom Penh. However, these rural trainees faced difficulties in accessing digital training programs, including poor internet connectivity, a lack of familiarity with videoconferencing services and less familiarity with device functionality. To this final point, at least one trainer mentioned that participants in interactive sessions struggled to view video content and follow tutorials simultaneously across multiple applications on the same device.

### *2. Key stakeholders – including the government, training providers and content creators – do not adequately disseminate or exchange information on important issues, content and players in the ecosystem.*

Interviewees mentioned barriers to gathering information on digital training initiatives in Cambodia, due to a low volume of publicly available resources and a lack of structural information-sharing mechanisms amongst key stakeholders. Some interviewees did mention sharing information on an *ad hoc* basis through professional and personal relationships, though donor and trainer provider privacy policies often placed restrictions on report sharing. As the digital training ecosystem develops, there is a need for funders to design communications strategies to help spread public information and promote industry-

[20] Council for the Development of Cambodia, "The Council for the Development of Cambodia (CDC) : Who We Are."

wide knowledge transfer about digital literacy and digital security trainings. Interviewees specifically mentioned their interest in sharing information on:

- **The prevalence of cyberattacks in Cambodia**: There are no publicly available government statistics on cyberattacks in Cambodia. Therefore, the general public does not have an accurate understanding of the frequency or severity of these threats.
- **Available digital training materials and content**: Training providers rarely use content created by others unless it is provided by a donor. While training providers often prefer using personally branded content, several stated that they would be interested in using or promoting other organizations' content if they could add their own personal branding. However, this can be difficult if they are not funded by the same donor.
- **Digital skills training programs**: Interviewees were often unaware of other programs operating in the digital skills training space and lacked a means of discovering them, other than word of mouth.
- **Digital hygiene best practices for CSOs:** According to interviewees, training providers lack data and examples that demonstrate how other CSOs have successfully transferred digital skills and knowledge to trainees. They also lack relevant examples of other CSOs successfully dealing with digital threats that could be integrated into their curricula or internal digital security trainings.

### *3. Many CSOs lack a permanent and trusted IT staff member.*

CSOs in Cambodia rely heavily on certain digital tools to conduct their work. However, many lack in-house IT staff. As interviewees explained, this could be the case for a few reasons: first, donors or funders often deny IT funding requests to save on costs. Second, CSOs might not recognize the importance of hiring a dedicated IT staff member. Having a knowledgeable, trusted internal IT team (or staff member) is a crucial part of ensuring good digital hygiene at the organizational level. While part-time or shared resources can help CSOs meet certain IT needs, not having at least one fully dedicated staff member leaves CSOs more vulnerable to cyberattacks. One digital security expert mentioned that organizations should ideally have one IT person for every 15 employees in order to properly monitor activity across 30 devices (laptops and phones) and manage risks in real time.

### *4. CSOs lack internal trainings about digital literacy and security and do not have access to external trainings tailored to their needs.*

Overall digital hygiene among CSO staff is often poor. This highlights the importance of educating all staff members on important digital security topics to build organizational IT capacity. CSOs do not have access to digital capacity building opportunities, largely due to their lack of internal trainings (internal IT capacity) and access to external trainings tailored to CSOs needs. CSOs require training specifically on digital security topics. However, the current digital literacy and security training landscape in Cambodia does not include programs that holistically address these areas.

Based on interviews, digital hygiene trainings for Cambodian CSO staff tend to focus on technical skills and general best practices, rather than judgment and critical thinking - "soft skills" that bridge the gap between simply understanding the basics of digital security topics and actually exhibiting safe behaviors in practice. Cambodia has a limited number of digital literacy and security programs targeting professional and citizen journalists (a group that share some similarities with CSO staff) that teach data, media and information literacy, including identifying mis- and disinformation. However, not all the content is relevant for CSOs - these programs heavily focus on writing and production skills, as well as journalist-specific social media use. These programs also do not typically focus on digital security, an important topic for CSOs.

Further, some interviewed CSOs provide minimal internal digital security training for their staff, either due to a lack of resources (some have no permanent IT staff, as outlined above), not prioritizing digital security, and/or a dangerous assumption that staff are already well-versed in IT and cybersecurity issues.

Organizations that do conduct digital security training for their staff are often local branches of larger international NGOs or organizations where technology is core to their mission. Some common digital security training topics include:

- Use of strong passwords and multi- or two-factor authentication
- Identifying and flagging potential business email compromise (BEC) emails including phishing, ransomware, e-commerce data interception, crimeware-as-a-service (CaaS), and cyber fraud
- Evaluating sources and fact-checking against fake news; and
- Understanding the social and legal consequences of posting content online.

Interviewees mentioned receiving training on other critical security items such as ransomware and viruses much less frequently, and typically only if they or their organizations have experienced these issues firsthand. This suggests that CSOs may be approaching digital security reactively rather than proactively.

## Recommendations for USAID and Other Funders

### *1. Increase programmatic investment outside Phnom Penh.*

In the long term, increased investment in widespread digital training can address gaps in local capacity, resulting in a larger digitally literate population capable of using computers and operating safely online. However, regional disparities should not be a deterrent to increasing programmatic investment in the short term, as there are effective ways to expand awareness of digital literacy and security topics due to high mobile internet penetration in rural provinces. Some options for reaching CSOs in rural provinces include:

- **Systematizing *ad hoc* training programs:** *Ad hoc* trainings currently provided outside Phnom Penh take place infrequently and for short periods of time. Existing training programs can create additional hubs in rural provinces to increase reach and provide greater access to digital upskilling opportunities.
- **Traveling conferences:** Traveling conferences can raise awareness of digital literacy and security issues in more remote regions of Cambodia without committing permanent resources to these areas. One example is BarCamp, a pop-up conference previously held several times a year across Cambodia to promote awareness of digital technology. However, BarCamp has been inactive since the beginning of the COVID-19 pandemic in Cambodia.
- **Public information campaigns:** A recent report published by the American University of Phnom Penh suggests a public information campaign in the provinces could help individuals better understand possible cybersecurity threats, vulnerabilities, and appropriate measures they can take to minimize risk.[21]

### *2. Support knowledge sharing among key stakeholders.*

High-level funders can provide or encourage the creation of mechanisms for information sharing and knowledge transfer among key stakeholders. For example, they can foster clear communication around which data and reports are private and which can be shared among CSOs and other individuals and organizations working on digital literacy and security. Ideally, as much information as possible would be made publicly available to relevant industry stakeholders. The creation of specific information-sharing mechanisms such as

[21] Corrado, Riccardo, and Morokot Sakal, "Cybersecurity in Cambodia: Awareness as a First Step."

websites, newsletters, industry conferences, roundtables, and associations could also encourage regular communication between stakeholders. Some organizations, such as the Asian Media Information and Communication Centre (AMIC), have already made limited attempts to create more formal communication mechanisms like these. Funders can also elevate, establish, and fund multiple activities to test which of these efforts best facilitate knowledge transfer in the CSO space.

Greater information and knowledge sharing among relevant stakeholders could help improve programming, increase transparency, and potentially bring more funds into Cambodia's digital development space. Training providers could make better programming decisions if they had access to updated information on prevalent and/or emerging cyber threats. Regular sharing of best training practices and examples of successful curricula can help make the entire digital training ecosystem become better informed and more effective in transferring digital knowledge and skills across Cambodia.

### *3. Allocate more funding for IT staff.*

Many Cambodian CSOs have a clear, urgent need for upgraded internal IT capacity, specifically for a full-time IT staff person who can build trust by maintaining an ongoing relationship with staff members. Funders and donors have an opportunity to address this need by allocating more funding for IT staff either by approving project-specific IT staffing requests or approving budgets with higher overhead rates to enable CSOs to hire organization-wide IT staff. While having permanent, full-time IT staff is ideal, a part-time staff member could be sufficient in light of funding limitations. Finally, funders could require that all organizations applying for funding have demonstrated access to IT expertise, which could lead to improved digital hygiene practices across Cambodia's CSO community.

### *4. Fund and support internal and external IT training programs for CSOs.*

CSOs can further lower their risk of falling victim to digital threats by ensuring that all staff are adequately trained on important digital literacy and security topics. While IT personnel can implement these trainings, access to external trainings is necessary for CSOs that lack these internal resources. Funders have an opportunity to fill these gaps by funding IT capacity-building initiatives.

One option is to fund and/or partner with existing digital literacy and security training programs (see Appendix A for program landscape) to create curricula that meet the specific

needs of Cambodian CSOs and nonprofits. Funding local training programs that lack the resources to expand program offerings is a good place to start, as these organizations understand the local context and already have training experience and materials that they can adapt for a CSO audience.

Another option is to provide funding and program deployment support for multinational organizations that run digital literacy or security programs not currently available in Cambodia. CSOs will need thoughtfully designed training curricula that recognize the sensitive nature of their work to ensure staff fully understand how to protect themselves and their organizations online. As such, localizing the training materials to Cambodia and Cambodian CSOs will be a critical component of this work.

Finally, funds could be channeled toward individual Cambodia-based consultants or content creators to design entirely new programs or curriculum tailored to Cambodian CSOs and nonprofits. Programs and curriculum geared toward CSOs will need to be tailored to the appropriate skill level and digital capacity needs.

## DIGITAL TRAINING PROVIDERS AND INDIVIDUAL CONTENT CREATORS

The following findings and recommendations are most relevant to ISAC and other training providers. Training providers refer to organizations that provide formal digital skills trainings, such as InSTEDD iLab Southeast Asia and The Idea Consultancy, but many items will also be relevant for individual trainers, consultants, or content creators who want to educate people on digital literacy and security. While this section focuses on digital training programs designed for CSOs, providers targeting different audiences such as children or MSMEs could also use much of this information.

### Findings:

#### *1. Low pre-existing digital literacy and critical thinking limit the effective transfer of digital literacy and security skills and knowledge.*

The majority of training providers interviewed expressed difficulty in effectively transferring digital skills to trainees, and post-training follow up often revealed that few trainees were regularly applying the skills and concepts taught during training. Interviewees frequently cited the limitations of pre-existing digital literacy and critical

thinking skills as a barrier to effectively teaching digital skills and hygiene. For example, some trainers reported having to regularly slow their pace or cover additional material once they realized that trainees lacked certain foundational digital skills. One interviewee in particular recalled needing to explain basic computer functions like opening an internet browser window before reverting back to the higher-level skill being taught. Non-digital natives without previous technical experience typically required remedial digital skills training with greater frequency and struggled to transfer digital skills between platforms and contexts. Digital natives may require less training on how to use any one device or platform. However, this does not mean that they are equipped to be safe online - they still need training on cybersecurity judgment, intuition, and relevant laws and regulations.

Some trainers reported needing to explain the importance of digital literacy and security skills, as many trainees did not expect to use these skills outside a professional setting or did not feel incentivized to learn about online threats unless they had previously fallen victim. Trainers also indicated that trainees were less likely to continue using digital skills if the curriculum did not include hands-on practice and/or included vague or impersonal examples. Many interviewees expressed skepticism about the efficacy of programs that only use lecture or video content, as they do not grant learners the opportunity to ask clarifying questions or cultivate proactive critical thinking skills. Using hands-on examples specific to the group's professional and/or personal experiences helped keep participants' attention and facilitate the transfer of skills.

Finally, the shift to online trainings during COVID-19 lockdowns further exacerbated challenges for effectively transferring digital skills and knowledge. Trainers saw a lack of engagement with online learning as a pervasive issue, particularly for non-interactive lecture content - one interviewee went so far as to question whether students were interested in learning online at all. In response, instructors who moved their programming online often made adjustments to combat fatigue, such as shortening sessions or splitting them between multiple days. Given the high likelihood of ongoing videoconferencing in the training ecosystem, strategies to actively engage trainees virtually are increasingly important.

### *2. Training providers experience difficulties assessing trainee progress and skill retention.*

Follow-up to assess trainee progress and skill retention requires sufficient time and resources, but many training providers have small teams and limited funds. These organizations facilitate trainings with only one or two staff members while working within a fundraising ecosystem that often optimizes for training class size without similar

incentives for promoting long-term quality interactions. Additionally, interviewees that did conduct follow-ups cited additional challenges in soliciting responses to evaluations and phone calls from trainees - some trainers mentioned having to reach out multiple times to get responses from participants. These issues highlight the importance of creating follow-up mechanisms that fit the training program's staff capacity and also proactively monitor participant progress and reinforce newly learned skills and behaviors.

Hosting training programs online enabled some organizations to increase the overall size and geographic reach of their training programs. However, this increase in scale reduced the amount of individual attention that learners received and made it incrementally more difficult to assess their progress towards learning objectives.

### *3. Training providers do not take advantage of pre-existing content.*

The majority of organizations and content creators interviewed created their own curriculum, though some were mandated to use materials provided by an external funding organization (such as Meta). Those who did create their own content were expressly motivated by a pride in their work and typically built out content/curriculum based on their own professional experience conducting digital training programs. Though international programs, private companies, and governments around the world have devoted huge amounts of resources towards developing effective digital training materials, very few interviewees used or were even able to identify sources of other usable content for trainings.

Beyond a lack of awareness, a couple of interviewees shared that other content creators were hesitant to use international materials due to translation and localization challenges. Translating and localizing content takes time and resources, and not all concepts can be easily adapted. For example, a recent report found that "the Western concept of privacy is not translated easily into the Cambodian (Khmer) language"[22] and as a result, many Cambodian users opt to use the English version of Facebook and memorize the features within the app.[23] This creates challenges for those users when new updates are released and features are moved around within the app. This can potentially jeopardize users' safety if a user unknowingly modifies a setting that applies to their data or privacy preferences. This suggests that "conversations and education about using Facebook safely in Khmer language often entail substantial definitional and translational work."[24]

[22] ICTworks. "Facebook Data Privacy Concepts Do Not Translate in Cambodia."

[23] Margaret, Sovannaroth and Dell, "Privacy Is Not a Concept, but a Way of Dealing with Life."

[24] ICTworks. "Facebook Data Privacy Concepts Do Not Translate in Cambodia."

However, translating and localizing international content may be less work than creating a new program from scratch, and the resources saved could be spent on other program-related activities. Though it still requires language translation, more culturally relevant content is available from other Southeast Asian countries.

### *4. CSOs often do not understand the laws and regulations applicable to their work.*

Several interviewees stated that CSOs and online users often lack an understanding of regulatory topics. Interviewees generally agreed that CSOs with an online presence require training on legal and regulatory topics related to their online activity. One technical expert interviewed expressed concern over organizations being punished for not understanding how to comply with these rules. CSOs still need to understand how legal and regulatory considerations in Cambodia's digital realm may affect their daily work.

## Recommendations for ISAC and Other Training Providers

### *1. Promote hands-on and relevant learning over memorization.*

Hands-on and scenario-based learning can elicit critical thinking, ensure that participants understand the "why" behind concepts being taught, and promote a broader understanding of how and when to apply these skills. Trainers can supplement lecture-style trainings with interactive opportunities for learners to practice their newfound skills - interviewees suggested dedicating 30-50%+ of training time to these activities.

Another effective teaching device is storytelling, where technical content is incorporated into a narrative to make it more tangible and emotionally engaging. Instead of using lecture slides to explain a step-by-step technical process, the trainer can introduce a hypothetical situation where characters need to go through the process to accomplish a task. Along this journey, natural decision points will provide an opportunity to engage learners by asking for their thoughts or suggestions while also identifying areas that need further instruction. For non-digital native trainees in particular, this step-by-step training on how to set up and use digital technology makes the training more approachable and increases the likelihood that participants continue using the skills after the training ends.

In addition to storytelling, individual or group projects and assignments are also a popular and effective component of many interactive training programs. This is particularly true when the work is directly applicable to learners' lives - for example, several interviewees

who had trained journalists mentioned assigning a final deliverable in the form of a news article to assess how well participants applied what they had learned. Hands-on learning exercises like these have the additional benefit of helping to assess whether participants can effectively apply newly learned digital skills. Limited digital literacy and critical thinking abilities make knowledge transfer difficult, but creating training content specific to trainees' lives can increase the likelihood that skills are acquired and continually used.

The emergence of online trainings during the COVID-19 pandemic made it even more difficult to keep trainees engaged and facilitate knowledge transfer. For organizations seeking to include a virtual component in their trainings, it is important to place a strong emphasis on ensuring that learners are able to ask questions and interact with content in a constructive way. By ensuring that its trainers incorporate relevant, interactive content, ISAC can improve engagement and knowledge transfer in future online training courses.

### *2. Focus on training both hard skills and intuition.*

Both digital literacy and digital security training programs typically include content on how to use relevant hardware and software, but it is important that digital security curricula are deliberately designed to foster judgment and critical thinking skills. It may be more difficult for learners to see the value in exercises that teach soft skills like decision-making: unlike learning to use a new tool, developing intuition does not give them a hard skill they can immediately put on their resume or demonstrate to others. However, staff members must be trained to be constantly vigilant, understand *why* certain actions are preferable to others, and be aware of potential consequences. Situational exercises provide one opportunity to walk participants through a real-life security scenario and test their abilities to make the right decision - for example, when deciding which online information to include in an article or report.

Digital security training program providers should also include content that emphasizes the breadth of potential digital security issues that CSOs may encounter. Adding case studies on digital security breaches that employees of similar organizations have experienced - or even highlighting gaps in preparedness within trainees' own organizations - can help communicate the importance of staying vigilant about these risks at all times. For example, a large multinational company in Cambodia reinforced the need for additional security training by sending employees a fake phishing email and internally reporting the percentage of employees who clicked on the links. Trainers can also explain the importance of digital security by showing how digital threats extend to their family, friends, and community. One option is providing a framework for analyzing these threats through a digital health check - a graphic or list that illustrates various types of online threats that

exist within a trainee's community and strategies to defend against them. These digital health checks can expand a trainee's understanding of digital security to new topics and raise awareness on how they can help protect other family members.

### *3. Use follow-up mechanisms to assess and reinforce behavior change.*

With COVID-19 driving many trainings online, follow-up became even more important for training providers to track participant learning outcomes and progress. Interviewees reported using one or a combination of the following evaluation and follow-up mechanisms to track participant progress:

- **Surveys:** Several interviewees mentioned administering a survey immediately after a training and, in some cases, a follow-up survey one to three months after the training. Quality surveys include specific and targeted questions, rather than open-ended ones, so training providers can gather information and data points to track progress and design future programming. Additionally, training providers might gain richer insights if surveys are paired with a knowledge application (deliverable) or recall mechanism (real-life security scenario) as outlined above.
- **Mentorship or coaching**: Many organizations mentioned that coaching and ongoing mentorship can increase retention, and those with staffing capacity have tried to incorporate some form of this into their programming. Training providers might consider offering optional, supplemental one-on-one or small group coaching sessions that give personalized support for participants.[25] These sessions are most helpful for participants who have specific, targeted questions about concepts learned during formal training or how to apply them to their work. They are also beneficial for those who simply need individual assistance setting up certain security tools, such VPNs or MFA. For example, InSTEDD iLab's MSMEs Digital Upskilling program offered participants multiple post-training coaching sessions; InSTEDD's recent report noted that nearly half the participants attended all the sessions, and roughly one third attended at least one.[26] Active participants reported finding the sessions very useful and relevant to their work.[27]
- **Volunteer help desk**: Another option for training providers is to recruit volunteers and create a help desk available to participants post-training. Organizations can use proactive outreach and outbound calls to remind participants to apply their newly learned skills while also evaluating their progress and providing insights on

[25] InSTEDD iLab, "MSMEs Digital Upskilling in Cambodia."
[26] Ibid.
[27] Ibid.

learning outcomes to training providers. Recruiting young, digital native university students to assist training staff could help scale up operations in exchange for providing an opportunity to work directly with important digital literacy and security concepts.

- **Social Media Groups***:* Training program staff who do not have the time or capacity to provide coaching or mentoring sessions can connect with trainees through Facebook or Telegram groups. This allows them to keep an open line of communication with participants who can reach out for help if/when they need it.

ISAC and other training providers can improve learning outcomes by adopting a combination of these evaluation and follow-up mechanisms to meaningfully engage participants post-training.

### *4. Carefully adapt international content for local audiences and invest in producing high quality Khmer language training materials.*

To reduce unnecessary content duplication, training providers could lean on existing resources and channel their efforts toward carefully translating and contextualizing important concepts from international content. Digital security measures like password protection, MFA, and VPNs are universal and do not change across countries. This makes it easy for training providers to pull technical information from trainings created in/for other countries and adapt them to the local context. Using successful programming from other areas or countries saves time and energy, while allowing the program to build on others' experience. The US, UK, Australia and Singapore are examples of places which have directly relevant, high-quality programming.

However, despite directly relevant international content, training materials still need to be localized for a Cambodian audience and reflect the specific digital literacy and security needs of the training audience. Cambodian digital security experts suggest that content recently developed in Malaysia and Thailand may have more culturally relevant material. Content will need to be tailored to reflect trainees' pre-existing skills and access to local digital infrastructure and CSO capacity. For example, a trainee is unlikely to practice or apply skills learned on a device that they cannot regularly access. Similarly, it will be critical that trainers frame terms in ways that resonate with participants, especially because certain concepts, such as cybersecurity and privacy, are difficult to translate from English to Khmer.

### *5. Include legal and regulatory content in digital security trainings.*

Training CSOs on digital regulations relevant to their work helps protect them against potential legal vulnerabilities. One concerned digital skills trainer suggested bringing a lawyer to digital security trainings to help educate CSO staff on laws, regulations, and policies relevant to their work. However, other interviewees noted that engaging trainees on dry, complex legal and regulatory topics could create its own set of challenges, as this content may be incrementally more difficult to communicate. The average CSO staff member does not need a fully comprehensive understanding of the legal environment - a general awareness about relevant regulations that apply directly to their work may be sufficient. To avoid overloading junior- and mid-level staff, it may be appropriate to save more comprehensive legal training for executive- or director-level staff for whom organization-level legal issues are immediately relevant on a daily basis.

### *6. Collaborate with key stakeholders to increase engagement, cross promote, and share best practices.*

While employers can mandate training attendance, active participation and engagement are much more difficult to elicit. Thoughtfully selecting a like-minded partner can help increase the perceived value of new digital literacy and security training programs and amplify outreach efforts. In addition to providing engaging content, a partnership with a recognizable brand or well-known industry expert can lend credibility if learners are less familiar with the organization conducting the training.

Some interviewees increased training attendance or engagement by working with trusted or well-known individuals or organizations to deliver their program, such as Meta, Microsoft, Google, and Smart Axiata. For example, one organization working with local journalists attracted more participants to its training by bringing in a trainer from a high-profile foreign publication. There are also a variety of local “influencers” - celebrities, social media personalities, entrepreneurs and security experts - who can lend excitement and credibility to training programs run by lesser-known organizations. Finally, in certain cases, the endorsement of government ministries can carry weight with the public. Two government ministries to consider are the Ministry of Post and Telecommunications (MPTC) and MoEYS, which are both active participants in digital development and digital security initiatives within the country.

# CONCLUSION

As Cambodians come online and interact with digital platforms with greater frequency, it is becoming increasingly important to ensure that Cambodians develop adequate levels of digital literacy and digital security skills. This is also true for Cambodian CSOs, who need a digitally literate and vigilant staff to maintain the online safety and reputation of their organizations. USAID and other funders have the opportunity to help build CSOs' digital capacity by allocating more funding for country-wide digital programming and IT trainings, as well as supporting knowledge sharing among key stakeholders. Similarly, ISAC and other training providers can strengthen CSO digital capacity by creating programs that promote critical thinking skills and reinforce healthy digital hygiene practices. By doing so, they will be providing vital support to the ISAC's overall goal of increasing social accountability for public service delivery and strengthening democracy and governance in Cambodia.

# APPENDIX A: DIGITAL TRAINING LANDSCAPE ASSESSMENT

## DIGITAL LITERACY AND SECURITY TRAINING PROGRAMS

| Program | Status | Organization | Delivery | Length | Key Topics/Skills Covered |
|---|---|---|---|---|---|
| ***Entrepreneurs/Micro, Small, and Medium Enterprises (MSMEs):***<br><br>Organizations that offer Cambodian entrepreneurs and MSMEs courses or workshops on content creation, social media advertising, e-commerce platform building, and other digital skills so that they can effectively use the internet to promote their business. | | | | | |
| Stronger Digital Campaign | Active | The Idea Consultancy | Online training + follow-up workshops (Zoom)<br><br>5 in-person trainings in Khmer | 3-hour initial training with 1 - hour follow-up workshops | Set up a social media page (especially Facebook); Photoshop and other digital marketing/branding |
| MSMEs Digital Upskilling | Active | InSTEDD iLab Southeast Asia | Online | 2 days of training followed by 3 coaching sessions | Enhancing passwords; Spam detection; digital marketing/branding |
| Digital literacy program | Active | SHE Investments | In-person + online (Google Meet and Zoom) | 8-day training | Digital writing in Google Docs & Sheets; Mainstream the use of Facebook into their business |
| Building Your Business's Online Presence | Closed | Impact Hub Phnom Penh | Online | 8-hour course | E-commerce, digital marketing/branding, digital rights management, data analytics |
| Go Digital ASEAN | Active | The Asia Foundation | Online | | E-commerce |

| | | | | | |
|---|---|---|---|---|---|
| She Means Business | Closed | PACT + Meta | Online | 0.5-1 day<br><br>4 modules in 2 sets<br><br>Seminar-style | Set up social media page (especially Facebook); Photoshop and other digital marketing/branding |
| **Program** | | **Organization** | **Delivery** | **Length** | **Key Topics/Skills Covered** |
| ***Education: High School/University Students***<br>Organizations that target high school and university students. They offer employment-oriented digital literacy and security trainings (e.g. website browsing, Microsoft, Adobe, password strengthening, etc.) | | | | | |
| Social impact program | Active | Digital Divide Data | Online (work-study program) | 6 weeks | Microsoft<br><br>Communication platform (i.e. Gmail/ Google Drive) |
| Adobe Training | Closed | Cambodia Children's Fund | Online (Zoom or Google meet) | 4-day curriculum with additional activities at STEM clubs | Graphic Arts, Production, Animation and Web Design through Adobe |
| Cyber Security Essentials | Active | IT Academy STEP | Online & in-person | 2.5 year professional course with students attending classes 3 days per week | Password strengthening; Anti-virus skill; Data privacy protection |
| ICT Angkor | Active | Cambodia Children's Trust | Online & in-person | One semester per each level | Email; Microsoft Office; website browsing; social media privacy; programming; robotics; web design; animation |
| Cybersecurity program | Unknown | Passerelles Numériques | Unknown | Unknown | Password strengthening; Anti-virus skill; Data privacy protection |

| | | | | | |
|---|---|---|---|---|---|
| Digital Literacy Program (a workshop targeting high school students) | Closed | Smart Axiata | in-person | 1-day training | Password strengthening; website browsing |
| **Program** | | **Organization** | **Delivery** | **Length** | **Key Topics/Skills Covered** |
| ***Journalism, privacy and fact-checking (Journalists, Nonprofits, CSOs)*** Organizations that offer journalists, nonprofits and CSOs trainings on using digital skills for storytelling, detecting disinformation and misinformation, and data privacy protection. | | | | | |
| Training on Data Literacy | Active | Open Development Cambodia | Online & in-person | 2-3 day training with following coaching sessions | Digital storytelling and data-driven visualizations |
| Information Literacy program | Active | Cambodian Center for Independent Media (CCIM) | Online | 3-4 day training | Disinformation and misinformation spotting; Digital storytelling |
| Internews program | Active | Internews | Online & In person | 1-3 day training with mentorship program | Digital storytelling; Password Strengthening; Data privacy protection; |
| Digital Rights Campaign | Closed | Transparency International | Online (Zoom & Google Meet) | 3-day training with additional practices | Digital storytelling; Social Media account management; Regulations on telecommunication |
| Digital Security Champions Project | Unknown | Cambodian Center for Human Rights | Unknown | Unknown | Digital Security; Data privacy |

## ADDITIONAL SOURCES OF KHMER-LANGUAGE DIGITAL LITERACY AND SECURITY CONTENT

| Content Creator | Background | Platform | Target Group | Key Topics/Skills Covered |
|---|---|---|---|---|
| Moses Ngeth | Digital Security Expert, formerly consulted for DAI on USAID's ISAC project | | Corporate clients: End-users and IT staff | Password manager; Microsoft Office 365; Email; OneDrive; VPNs |
| Chy Sophat | Digital Security Expert, formerly worked at InSTEDD and DAI on USAID's Development Innovations project | In-person; Facebook; Telegram; TikTok | Teachers; The youth; Citizen journalists | Cybersecurity; Data privacy |
| Ly Vandy | Digital Security Expert, Deloitte | In-person; YouTube; Client's internal platform | Corporate clients; The general public | IT governance; Cybersecurity: phishing, sexploitation, ransomware, viruses, account compromise |
| Si Em Fat | Transport Planning and Optimization Manager, Cellcard | Work with MPTC to make videos | Parents; Government agency | Cybersecurity; Online threats |
| Chumrum Digital | | Website; Facebook; Instagram | | Cybersecurity |
| USAID/DAI Online Safety Videos | Part of Digital Connectivity and Cybersecurity Partnership (DCCP) / Digital Frontiers program | Facebook | SMEs | Cybersecurity |
| CamCERT | Cambodia Computer Emergency Response Team | Website with blog posts / infographics | General public | Cybersecurity |

| | | | | |
|---|---|---|---|---|
| MyCERT | Malaysian Computer Emergency Response Team | CyberSAFE Malaysia website (posts, videos and games) | Children; youth; parents; general public | Cybersecurity |

# APPENDIX B: INTERVIEW QUESTIONNAIRE[28]*

General Digital Literacy and Security Questions:

1. How do you or your organization define digital literacy (digital security)?
    a. Which specific skills are most important?
    b. Hard and/or soft skills? (Technical vs Analytical skills)
2. How would you assess the overall digital literacy & security environment in Cambodia?
    a. What are the primary challenges and constraints in enhancing digital literacy in Cambodia?
    b. Which platforms or digital services do you consider most important? Are there important technical or infrastructure bottlenecks?

Organization Level Questions:

3. Can you please give a brief overview of your background and your role at [organization]?
4. Please give us a general overview of your organization and your work in Cambodia (both digital literacy-related and more broadly):
    a. What is your organization's mission?
    b. How do digital literacy and/or security gaps in Cambodia affect your organization's work?
    c. What knowledge, access or technical capabilities could help alleviate these issues?
5. General organizational facts (potentially save some for follow-up email):
    a. How many people are employed by your organization?
    b. How long do volunteers/workers typically work for your organization?
    c. What is the organizational structure? (horizontal, hierarchical, team-based, functional, divisional, etc.)
    d. Amount of funding: Who are your main donors and funding sources?
        i. Has your program received any financial or other support from any Cambodian government agencies, like MPTC or MoEYS?

Program-Specific Questions (if applicable):

6. Please give a general overview of your program, including overall purpose, skills taught, target demographic, number of participants, timing, cost and overview of activities.
    a. Qualitative:

[28] Special thanks to Paul Bahk, Jung Yu Chang and Suzie Zhang, who collaborated with the SAIS team to develop this template.

*This template was used as a tool to guide conversations. Not every participant was asked every question.

        i. What is the purpose of your project? What do you want to accomplish?
        ii. How do you attract participants?
        iii. How do you carry out the program e.g. onsite/online training?
        iv. Do you target/include certain demographics e.g. monks, females? Why?
        v. Why did these people join your program?
    b. Quantitative (to ask for in follow up email):
        i. Number of trainers/trainees (disaggregated by gender, age, education, household, employment)?
        ii. Cost of project: Who are your donors and funding sources?
        iii. Dropout rates (disaggregated by gender, age, education, household (?), employment)? Why did they drop out?
        iv. How many participants have graduated from your program?
7. Evaluation-related questions: Would you consider your program a success? Why or why not? What would you change if you were to run it again?
    a. How do you measure success for your program? Have you designed any evaluation mechanisms before implementing the program?
    b. What were some of the unexpected challenges you have faced? How did you resolve it?
    c. Any lessons learned from your project (positive/negative)?
    d. What are some of the feedback you have received from the program participants (positive/negative)?
    e. Employment/education outcomes after graduation?
8. When creating your program, which resources did you consult to develop the curriculum or training materials?
    a. What are the challenges you faced when consulting with certain resources e.g. private sector companies such as Microsoft and Google?
    b. Has your program received any financial or other support from any Cambodian government agencies, like MPTC or MoEYS?

Follow-Up Questions:

9. Are there any additional topics related to digital literacy or digital security that you think we should look into further?
10. Would you be willing to share your latest M&E report (if you have one)?
11. Are there any other organizations, companies, or donors that you think are doing good work in the digital literacy/security space in Cambodia?
    a. Do you have contacts of other related organizations?
    b. Do you have contact information of participants who have graduated from the program (and would be willing to speak to us)?

# BIBLIOGRAPHY


American Library Association (ALA). n.d. “Digital Literacy.” American Library Association. Accessed April 8, 2022. https://literacy.ala.org/digital-literacy/.

Banga, Karishma, and Dirk Willem te Velde. 2020. “Cambodia, Covid-19 and Inclusive Digital Transformation: A Seven-Point Plan.” SET. July 7, 2020. https://set.odi.org/cambodia-covid-19-and-inclusive-digital-transformation-a-seven-point-plan/.

Beschorner, Natasha, James Neumann, and Miguel Eduardo Sanchez Martin. 2018. “Benefiting from the Digital Economy. Cambodia Policy Note.” *World Bank Group*. https://doi.org/10.1596/30926.

Council for the Development of Cambodia. 2017. “The Council for the Development of Cambodia (CDC) " Who We Are.” Council for the Development of Cambodia (CDC). 2017. http://www.cambodiainvestment.gov.kh/about-us/who-we-are.html.

Corrado, Riccardo, and Morokot Sakal. 2021. “Cybersecurity in Cambodia: Awareness as a First Step.” Cambodia Development Center. August 5, 2021. https://cd-center.org/wp-content/uploads/2021/08/P124_20210805_V3IS11_EN.pdf.

DAI. 2021 “Year 2 Digital Assessment Key Findings.” DAI.

Eshet, Y. 2004. “Digital Literacy: A Conceptual Framework for Survival Skills in the Digital era.” *Journal of Educational Multimedia and Hypermedia* 13(1): 93-106. Norfolk, VA: Association for the Advancement of Computing in Education (AACE).

ICTworks. 2022. “Facebook Data Privacy Concepts Do Not Translate in Cambodia.” https://www.ictworks.org/facebook-data-privacy-concepts-cambodia/#.YmWNdy2ZMWo

Fenwick, Sam. 2021. “Cambodia, February 2021, Mobile Network Experience.” Opensignal. February 4, 2021. https://www.opensignal.com/reports/2021/02/cambodia/mobile-network-experience.

Heng, Pheakdey. 2019. “Preparing Cambodia's Workforce for a Digital Economy.” Konrad-Adenauer-Stiftung: Foundation Office Cambodia. September 13, 2019. https://www.kas.de/en/web/kambodscha/single-title/-/content/preparing-cambodia-s-workforce-for-a-digital-economy-1.

InSTEDD iLab. 2022. “MSMEs Digital Upskilling in Cambodia.” Phnom Penh: InSTEDD iLab. https://ilabsoutheastasia.org/wp-content/uploads/2022/01/MSMEs-Digital-Upskilling-Cambodia.pdf

Kemp, Simon. 2021. “Digital in Cambodia: All the Statistics You Need in 2021 - DataReportal – Global Digital Insights.” DataReportal. DataReportal – Global Digital Insights. February 11, 2021. https://datareportal.com/reports/digital-2021-cambodia.

Kem, Bora, Jolyda Sou, Zoë Ng & Penhleak Chan. 2019. “Startup Kingdom: Cambodia’s Vibrant Tech Startup Ecosystem In 2018.” National Institute of Posts, Telecoms & ICT and Smart Axiata. https://static1.squarespace.com/static/56a87acd05f8e263f7b16c7f/t/5c8a98caec212db15379299d/1552586969710/Cambodian_Tech_Startup_Report_Final_150319.pdf

LIRNEasia. 2018. “After Access: ICT access and use in Asia and the Global South.” Colombo: LIRNEasia. https://lirneasia.net/wp-content/uploads/2018/10/LIRNEasia-AfterAccess-Asia-Report.pdf

Ministry of Education, Youth and Sport (MoYES). 2019. “Education Strategic Plan 2019-2023.” UNESCO. https://planipolis.iiep.unesco.org/en/2019/education-strategic-plan-2019-2023-6764

Margaret C., Jack, Pang Sovannaroth, and Nicola Dell. 2019. “Privacy Is Not a Concept, but a Way of Dealing with Life.” *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–19. https://doi.org/10.1145/3359230.

Marshall, Stephen. 2021. “Cambodia - Telecoms, Mobile and Broadband - Statistics and Analyses - Buddecomm.” Cambodia Telecoms Market Report, Statistics and Forecast 2020 2025. June 30, 2021. https://www.budde.com.au/Research/Cambodia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses.

MPTC. 2022. “Home.” The Ministry of Post & Telecommunications . January 20, 2022. https://mptc.gov.kh/en/.

Plostins, Inta, Pounlok Sour, and Samnang Oung. 2020. “Innovations for Social Accountability in Cambodia Initial Digital Assessment.” DAI.

Sao, Vichheka, Anisha Ratan, and Hor Otdam. 2021. “Understanding How Young Cambodians Use Media and Information - Media Action.” BBC News. BBC. May 2021.

https://www.bbc.co.uk/mediaaction/publications-and-resources/research/briefings/asia/cambodia/klahan9-media-infographic-2021/.

Simplilearn. 2022. “What Is Digital Security: Overview, Types, and Applications Explained [Updated].” Simplilearn.com. Simplilearn. March 24, 2022. https://www.simplilearn.com/what-is-digital-security-article#:~:text=Digital%20security%20is%20the%20collective,biometrics%2C%20and%20secured%20personal%20devices.

Telecommunication Regulator of Cambodia (TRC). 2021. “Phone Subscriptions.” TRC. 2021. https://www.trc.gov.kh/en/mobile-phone-subcribers/.

United Nations Development Programme (UNDP). 2020. “Assessment of Digital Literacy for Employability and Entrepreneurship among Cambodian Youth: UNDP in Cambodia.” UNDP. September 25, 2020. https://www.kh.undp.org/content/cambodia/en/home/library/assessment-of-digital-literacy-for-employability-and-entrepreneu.html.

Vannak, Chea. 2018. “Funds Manage to Collect $4 Million for Development of Telecom Sector despite Non-Fulfilled Payments by Most Industry Players - Khmer Times.” Khmer Times - Insight into Cambodia. February 7, 2018. https://www.khmertimeskh.com/106880/funds-manage-collect-4-million-development-telecom-sector-despite-non-fulfilled-payments-industry-players/.