الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

Commencement of the National Initiative for Digital Safety

In its pursuit to strengthen cybersecurity standards and digital safety nationwide and within the community, the National Cyber Security Agency has introduced the 'National Initiative for Digital Safety.' This initiative aims to reach a wide range of the population, enhancing the stability of the nation's cyberspace and improving the community's ability to withstand rising cyber threats.

The initiative is the most extensive awareness project of its kind in the state, spanning three years. It employs a science-based approach to maximise its effectiveness and ensure successful realisation of its goals.

The initiative derives its importance from the need to stay aligned with global advancements in cybersecurity and digital safety, as well as the critical task of securing state institutions and various segments of society against increasing cyber threats, particularly given the rapidly evolving nature of these risks.

The initiative is based on a careful analysis of the current level of cybersecurity awareness among the target groups, identifying specific knowledge gaps within each one. It then addresses these gaps by delivering cybersecurity awareness content through various methods, including guides, training video games, informational booklets and videos, as well as field visits.

Dalal Al-Aqeedi
Director of National Cyber Excellence Department

The project... A sound scientific methodology in planning and execution

The success of any initiative or project relies on efficient planning, execution, and effective use of scientific research tools. The National Cyber Security Agency has prioritised this in its planning for the National Initiative for Digital Safety. A research-driven approach has shaped every phase, from identifying the target groups and selecting the most appropriate awareness tools to creating tailored content for each group within the initiative.

The scientific research methodology employed in planning the initiative is clearly demonstrated through the preparation of several detailed studies. This ensures complete reliance on research findings rather than personal judgement. Each target group of the initiative has been thoroughly analysed, with their general, educational, and cybersecurity characteristics carefully identified.

The selected awareness tools have also been thoroughly researched, and their effectiveness evaluated. Additionally, a comprehensive survey of the wider society was conducted to identify the knowledge gaps among the initiative's target audience and to determine the most suitable awareness content to address these gaps. At every stage of its planning, the initiative has been fully grounded in a sound scientific methodology, utilising advanced tools for research and statistical analysis.

Various Segments with Broad Reach

In its dedication to providing cybersecurity awareness content to various segments of society, the National Cyber Security Agency, through the National Initiative for Digital Safety, aims to reach a wide range of community groups. This effort contributes to strengthening cybersecurity resilience and improving digital safety standards. The initiative's effectiveness and impact are evident in its approach of delivering tailored awareness content to each segment, meeting their specific educational needs. This strategy enhances overall awareness of cybersecurity and digital safety concepts.

The initiative targets the following groups as part of its approach:

- The elderly
- Women and families
- University students
- Employees in the financial and banking sectors
- Individuals with special needs
- Civil society institutions
- Expatriate workers

Varied and Comprehensive Awareness Tools

To achieve the initiative's goals and realize its vision and mission, the National Cyber Security Agency is committed to delivering an integrated mix of awareness tools to the targeted segments. The National Cyber Security Agency effectively and efficiently communicates information by providing a diverse and comprehensive set of tools.

These tools were selected based on scientific research and a systematic analysis of their effectiveness, choosing the best combination by drawing on leading international practices and the relevant technology. This ensures that the awareness content reaches the targeted segments in an effective and efficient manner, contributing to the achievement of the initiative's goals and the fulfilment of its vision and mission.

The following are the awareness tools adopted within the initiative:

- Digital safety guides
- Printed awareness booklets
- Electronic awareness booklets
- Animated videos
- Awareness videos
- Cybersecurity awareness games
- Field visits

The Cyber Bulletin...

An Innovative Awareness Program

The National Cyber Security Agency prioritizes the promotion of creativity and innovation in the execution of the National Initiative for Digital Safety. Understanding that creativity and innovation are essential for success and achieving objectives, the agency is also committed to delivering awareness content through effective and innovative training channels.

The Cyber Bulletin is an innovative programme developed by the agency as part of the initiative. It consists of multiple animated video episodes, each of which addresses a cybersecurity issue relevant to one of the targeted segments. The programme's concept includes a cybersecurity expert who answers questions from the audience, represented by various animated characters. This programme stands out for its pioneering concept and creative execution.

Scientific Studies and Research Methodology

The National Cyber Security Agency has conducted five scientific studies, each focusing on a different aspect of the initiative, in line with the scientific research approach it adopted for planning and implementation. These studies are:

- Analysis of Cybersecurity Trends in the State of Qatar.
- Identifying the Key Participants (Target Audience) for the Initiative and Potential Partner Organisations.
- Assessing Current and Future Capabilities of Tools for Enhancing Cybersecurity Awareness and Digital Safety
- Leading Regional and International Expertise in Cybersecurity and Digital Safety.
- A Study of Digital Safety Activities in Leading Centres Worldwide.

Study One

Analysis of Cybersecurity Trends in the State of Qatar

To identify the cybersecurity knowledge gaps within different segments of society and assess the current level of awareness of cybersecurity and digital safety concepts, a survey was conducted using an electronic questionnaire distributed to the targeted segments of the initiative.

The collected data was then analysed statistically using SPSS software.

The main goal of this study was to understand the current trends in cybersecurity and digital safety in the country. The findings will guide the identification of the initiative's target segments and help tailor the most suitable awareness content for each group. To ensure comprehensive coverage of all segments of society, including both citizens and residents, whether Arab or non-Arab, the questionnaire was made available in both Arabic and English.

The statistical analysis of the data revealed knowledge gaps in the following areas among the targeted segments:

- General understanding of cybersecurity and digital safety.
- Safe internet browsing practices.
- Risks of cyber hacking.
- Risks associated with ransomware.
- Dangers of social engineering.
- Security of financial accounts.
- Risks of using public Wi-Fi networks.

In terms of awareness of cybersecurity and digital safety concepts, the study results were as follows:

33% — **The elderly**

37.1% — **Expatriate workers**

41% — **University students**

63% — **Employees in financial and banking institutions**

28% — **Women and families**

Second Study

Identifying the Key Participants (Target Audience) for the Initiative and Potential Partner Organisations

Adopting a scientific research methodology and academic standards, the initiative identified the general, cybersecurity, and training characteristics of its target segments. The goal was to determine the most effective combination of awareness tools for each segment, ensuring that the initiative delivers accurate and comprehensible scientific content tailored to each group's specific needs.

The National Cyber Security Agency and numerous state institutions have partnered to form the National Initiative for Digital Safety, which is considered a strategic project. This study, therefore, assessed the capabilities and expertise of each partner to define their roles within the initiative, with the aim of leveraging their strengths to support the agency's overall objectives.

Added Value of the Study

The study provides precise insights into the general and cybersecurity characteristics of each target segment, creating a valuable knowledge base that can be utilised both in implementing the initiative and in other related activities, programmes, or projects. Additionally, the study provides detailed guidance on how to deliver awareness content to each segment based on a scientific methodology that can be applied both within and outside of the initiative.

Furthermore, the study enhances the National Cyber Security Agency's ability to manage and coordinate its partners' contributions. Effective management requires a thorough understanding of each partner's expertise, their area of work, and their operational methods. This knowledge enables the agency to define the expected role of each partner and identify the best way to harness their potential.

The initiative's partners, as determined by the study's findings, are:

Civil Society Organisations

Qatar Computing Research Institute

Local and International Educational Institutions

Third Study

Assessing Current and Future Capabilities of Tools for Enhancing Cybersecurity Awareness

This study analysed the accumulated expertise of the National Cyber Security Agency, which will be leveraged in implementing the initiative. The agency has built up this expertise through its previous programmes and projects, including the Cybercrime Prevention Training Programme, the Cybersecurity Curriculum Project, the Cyber Echo school visits project, and the National Cybersecurity Training Programme.

The study also conducted a systematic analysis of the training tools adopted within the initiative, assessing the relative importance of each tool. These tools include digital safety guides, awareness videos, animation videos, printed and electronic awareness booklets, training electronic games, and field visits. The study then identified the most effective combination of these tools to ensure the initiative's success in achieving its objectives and fulfilling its vision and mission.

Moreover, the study examined key international cybersecurity and digital safety indicators and evaluated the initiative's expected impact on these indicators. By the end of the initiative, it is anticipated that Qatar's ranking on these indicators will improve, thereby enhancing the country's position in the global cybersecurity landscape. The studied indicators include:

- Global Cybersecurity Index
- Cybercrime Prevention: Capacity Building Assessment Tool
- Cyber Maturity in the Asia-Pacific Region
- Cyber Readiness Index 2.0 (CRI)
- Cybersecurity Capacity Maturity Model for Nations (CMM)
- Cyber Strategy Development and Implementation (CSDI) Framework
- Global Cybersecurity Index (GCI)
- National Cyber Assessment Framework (NCAF)
- National Cybersecurity Index (NCSI)

Fourth Study
A Study of the Best Regional and International Practices in Cybersecurity and Digital Safety

To benefit from the experiences of other nations in cybersecurity and digital safety, this study analysed the practices of 20 countries. It focused on identifying the most significant threats and examining the measures and plans these countries have implemented to address current and future threats. The study covered countries from North and South America, Europe, Asia, and the Arab world.

Importance of Studying National Experiences

All countries face similar cyber threats, with attackers often using the same tools and methods. Therefore, studying other countries' cybersecurity experiences is essential to understand the threats and risks they face, as well as the strategies they use to counter security breaches. This analysis helps identify the strengths, weaknesses, advantages, and disadvantages of each country's approach.

The study included the following countries:

American Countries	European Countries	Asian Countries	Arab Countries
• The United States	• The United Kingdom	• South Korea	• Saudi Arabia
• Canada	• France	• Russia	• The United Arab Emirates
• Brazil	• Germany	• Singapore	• Oman
	• Italy	• China	• Egypt
	• Norway	• Iran	• Morocco
			• Bahrain

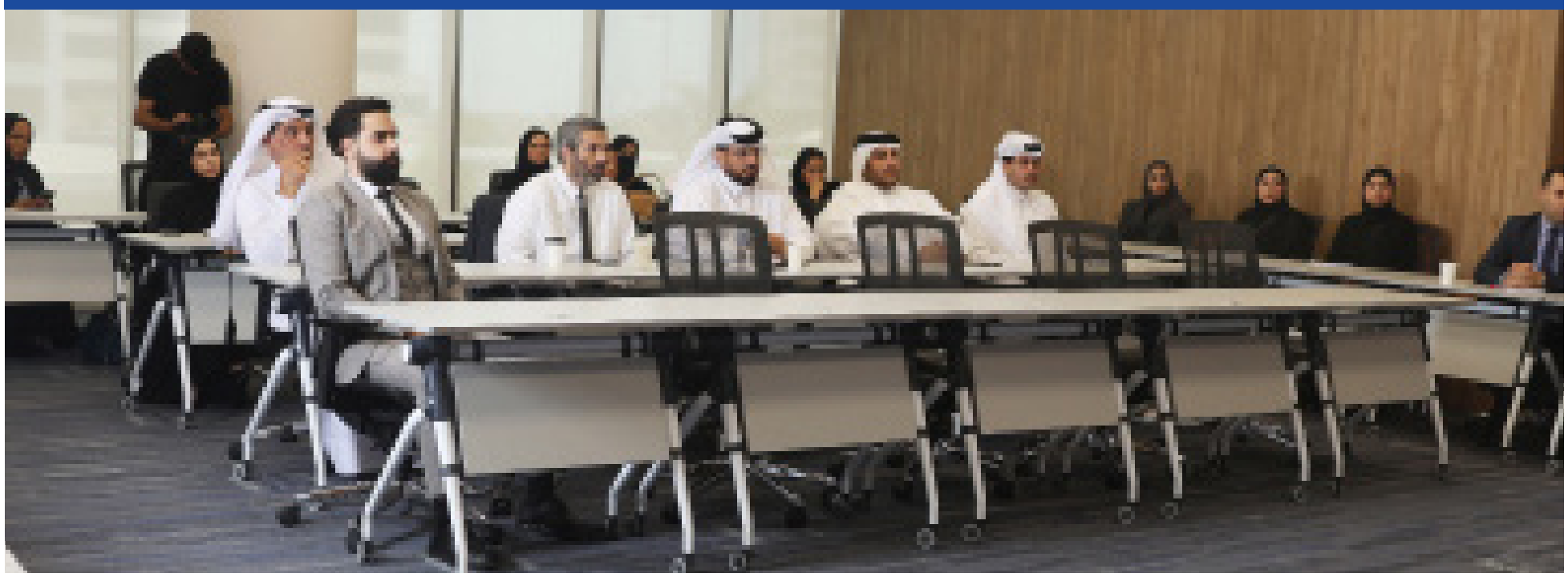
Fifth Study

Leading regional and international expertise in cybersecurity and digital safety

Recognising the importance of scientific research in cyberspace and the need to stay informed about modern cybersecurity research trends, this study has examined the methodologies of the leading international cybersecurity research centres. It has also assessed their scientific output in terms of quantity and quality, as well as identified their strengths and weaknesses. The goal is to leverage the insights gained from these centres to enhance the initiative, helping it to succeed and achieve its broader goals.

During the study, the methodologies of 15 international cybersecurity research centres were analysed. The added value of the study lies in its ability to extract key findings from cybersecurity research and apply them to the initiative's practical tools.

Furthermore, the study's added value extends beyond the initiative itself, encompassing projects and initiatives outside its immediate scope, including activities and events organised by the National Cyber Security Agency. It also serves as an information resource that can be utilised to support the implementation of the initiative's activities and to identify the most up-to-date cybersecurity awareness content.



Contact National Cyber Excellence Department

00974 404 663 79
00974 404 663 63
https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa