الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

With the aim of enhancing the stability of national Cyberspace and establishing a secure digital environment:

The National Cyber Security Agency is conducting its first field visit as part of the National Initiative for Digital Safety.

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

As a demonstration of the notable efforts led by the National Cyber Security Agency to enhance digital safety standards across the state, support the stability of cyberspace, and establish a secure and efficient digital environment for individuals and business enterprises alike, the agency has introduced the National Initiative for Digital Safety, which adopts a preventative approach to addressing cyber risks. As part of the efforts of this initiative, the National Cyber Security Agency is conducting its first field visits, which focus on improving cybersecurity competence among the targeted community segments.

The National Initiative for Digital Safety comprises a diverse range of activities dedicated to awareness-raising, training, and education in the fields of digital safety and cybersecurity. It targets the wider community across all age groups, social segments, educational backgrounds, and professional sectors, thereby contributing to the sustainable positive impact the initiative aims to achieve in enhancing public awareness of cybersecurity. The initiative's activities address the latest developments and issues in digital safety, the principles of responsible and secure Internet use and various technological applications, the adoption of emerging technologies, and the potential cyberspace threats.

The initiative is one of the National Cyber Security Agency's key initiatives to raise public awareness, based on its role in ensuring the security of cybersecurity across the state as the authorised national authority responsible for this field. In planning and implementing the initiative, the agency adopted the most up-to-date, internationally recognised standards for cybersecurity awareness, complemented by the policies and frameworks of leading international organisations concerned with cybersecurity and digital safety. These efforts are aligned with the cultural identity and social values of Qatari society and support the objectives of the National Cyber Security Strategy and Qatar's 2030 Vision.

In the first week of field visits, ... institutions were visited, awareness content was delivered to ..... participants, and ..... gifts were presented to them.

«The National Initiative for Digital Safety »

is ambitious and strategic

The primary mission of the National Cyber Security Agency is focused on achieving a range of national strategic objectives. A primary objective is the creation of a secure digital environment in Qatar for all, including children, families, senior citizens, and employees across both public and private sector institutions. In alignment with this approach, the agency is actively engaged in planning and implementing long-term strategic initiatives and projects, whose primary outcomes aim to bring about significant change in public awareness of cybersecurity and digital safety standards, enhance the digital environment across both the public and private sectors, and empower individuals and business enterprises to use technology efficiently, effectively, and securely. These objectives are not limited to a specific timeframe; rather, they are long-standing priorities that the agency regularly pursues.

Eng.
Abdulrahman bin Ali Al Farahid Al Malki
President of the National Cyber Security Agency

As a strategic and ambitious project of the Agency, and in accordance with its framework, the National Initiative for Digital Safety has been meticulously planned and implemented in line with the latest international trends. It aims to bring about significant digital and behavioural transformation within the targeted segments of society, enabling them to maintain positive and secure use of technology. In this way, digital safety becomes not merely a topic of public awareness but a way of life and a practical framework that contributes to establishing a sustainable collective awareness across Qatari society.

The initiative is the largest awareness-raising project in the state, extending over a three-year period. It adopts a research-based methodology that enhances its effectiveness and ensures the achievement of its strategic objectives. The initiative is vital to keeping up with global cybersecurity trends and protecting government bodies and the public from the rising risks of cyberattacks, especially as these threats grow more sophisticated.

The initiative is based on a clear approach that begins with an in-depth assessment of cybersecurity awareness levels across the targeted groups. It identifies specific knowledge gaps within each group and addresses them through tailored awareness content delivered using various methods, including cybersecurity guides, interactive training games, booklets, awareness-raising videos, and field visits.

The National Initiative for Digital Safety delivers a positive impact and a sustainable outcome

The National Cyber Security Agency has consistently prioritised sustained impact in its response to cyber risks and in its efforts to raise cybersecurity awareness and build capability across society. This commitment means ensuring that the effect of each project or initiative does not end upon its completion. This strategic focus is clearly demonstrated across the range of programs and initiatives adopted by the Agency—from the Cybercrime Prevention Training Program to the Educational Cybersecurity Curriculum Project and the school field visits project Cyber Eco, and through to the National Cybersecurity Training Program. In each of these initiatives, the Agency has applied an approach designed to generate long-term positive outcomes on national awareness of cybersecurity and digital safety. This same approach is reflected and reinforced within the National Initiative for Digital Safety.

The methodology adopted by the Agency in planning and implementing the initiative is based on the integration of a comprehensive set of awareness tools, designed to complement and reinforce one another to ensure sustained impact across all targeted segments. The content provided within the initiative is also characterised by coherence and integration—an approach that serves as a primary mechanism for preserving the initiative's effectiveness beyond its conclusion. This integrated methodology underscores the importance of the initiative and its contribution to strengthening the stability of national Cyberspace.

Mr. Khaled Al Hashimi
Director of National Cyber
Enablement and Excellence Affairs

The Initiative:

A Comprehensive Scientific Method in Planning and Delivery

The success of any initiative depends greatly on how effectively and efficiently it is planned and executed, as well as on the use of sound scientific research methods. This principle has guided the National Cyber Security Agency in developing the National Initiative for Digital Safety.

From the outset, the Agency followed a structured, research-driven methodology through every stage of planning—beginning with the identification of the initiative's target groups, the selection of the most suitable awareness tools, and the design of tailored content for each audience segment.

This approach is evident in a series of scientific studies carried out to ensure that all planning decisions were grounded in research rather than personal judgment. Each target group was analysed to identify its general characteristics, educational needs, and cybersecurity profile. Likewise, the effectiveness of the awareness tools was thoroughly assessed. A national survey was also conducted to pinpoint knowledge gaps within the target audience and guide the development of appropriate awareness content to address those gaps.

At every stage, the initiative has been built on a comprehensive scientific foundation and supported by modern research and statistical analysis tools.

Dalal Al-Aqeedi

Director of the National Cyber Excellence Department

The National Initiative for Digital Safety

Diverse Groups and Broad Engagement

As part of its commitment to delivering cybersecurity awareness content to all segments of society, the National Cyber Security Agency, through the National Initiative for Digital Safety, aims to engage a wide range of the community. This approach contributes to enhancing cybersecurity resilience and improving digital safety standards.

The effectiveness of the initiative and its ability to create impact are demonstrated through the delivery of tailored awareness content to each group, aligned with their specific needs. This, in turn, positively influences public understanding of cybersecurity and digital safety concepts.

In line with this approach, the initiative targets all segments of society, with a particular focus in the first year on the following groups:

- Senior Citizens
- Women and Family
- People with special needs
- University Students
- Expatriate Workers
- Civil Society Organisations
- The Financial and Banking Sector

Focus Areas That Address the Knowledge and Training Needs of Targeted Groups

The international community is experiencing unprecedented and rapidly accelerating technological developments. These advancements are directly associated with a growing level of cyber threats that affect individuals, institutions, and societies regardless of their level of economic or social progress. This situation necessitates enhancing public awareness of cybersecurity and digital safety principles and improving the ability of individuals and business enterprises to interact with technological tools and internet applications in a safe and responsible manner.

In response, the National Cyber Security Agency has prioritised the integration of comprehensive focus areas within the National Initiative for Digital Safety. These focus areas are designed to meet the knowledge and training needs of all targeted groups in the cybersecurity domain. The initiative addresses these needs through a variety of activities and engagements, which include, for example, awareness booklets, visual content, instructional guides, and cybersecurity-based educational games.

In general, these focus areas cover the following topics:

- Cybersecurity and digital safety
- Principles of safe internet use
- Responding to cyber threats
- Digital data privacy
- Modern cybersecurity concepts
- Artificial intelligence and advanced cyber threats
- Cybersecurity and digital safety strategies
- Digital safety for children
- Cybersecurity for institutions
- Cybersecurity for families
- Ethical principles in cyberspace
- Social and ethical standards online
- Digital legal literacy

Diverse and Integrated

Awareness Tools

To realise the objectives of the initiative and fulfil its vision and mission, the National Cyber Security Agency is committed to reaching the targeted segments of the initiative through a well-integrated mix of awareness tools. By offering a variety of complementary tools, information can be delivered effectively and efficiently.

These tools have been selected based on scientific research and systematic analysis of their effectiveness. The most suitable combination was chosen by referencing leading international practices and assessing the technical characteristics of each tool. This approach ensures that cybersecurity awareness content reaches the targeted groups with both impact and efficiency, contributing to the achievement of the initiative's goals and the realisation of its overall vision and mission.

The following is a list of the awareness tools adopted under the initiative. These tools and activities include, but are not limited to, the following:

Cybersecurity games

Awareness booklets

Theoretical awareness content

Gifts

Awareness workshops

Innovative educational games

Scientific Studies and Structured Research Methodology

In line with the scientific research methodology adopted by the National Cyber Security Agency in the planning and implementation of the initiative, five scientific studies were developed, each addressing a specific dimension of the initiative. These studies include the following:

A Study of Digital Safety Activities in Leading Centers Worldwide.

Leading regional and international expertise in cybersecurity and digital safety.

An assessment of the current and anticipated capabilities of the tools needed and available to enhance digital safety awareness.•

Identifying the key participants (target audience) for the initiative and potential partner organisations.

Analysis of Digital Safety Trends in the State of Qatar.

The Digital Safety Guide:

Principles for Safe Engagement with Emerging Digital Developments

As part of its ongoing efforts to enhance Qatar's global standing and leadership in international cybersecurity rankings, the National Cyber Security Agency launched the National Initiative for Digital Safety as a central pillar supporting national efforts aligned with Qatar National Vision 2030.

In terms of the awareness tools and techniques adopted within the initiative, the Agency placed strong emphasis on diversity and relevance. Among the most impactful of these tools are the instructional guides, particularly the Digital Safety Guide.

The Digital Safety Guide is a practical, instructional resource based on the National Cybersecurity Awareness Framework. It serves as an interactive tool designed to help different targeted groups engage with the internet, technological applications, and emerging digital and cyber developments in a safe and responsible manner. Accordingly, a dedicated version of the guide was developed for each group, adapted to its specific knowledge level and social context.

The guide provides an overview of various cyber threats that individuals may encounter during their everyday use of the internet and digital tools. It also offers practical tips and general recommendations on how to respond to cyber threats safely, promptly, and effectively—particularly those targeting personal data, online accounts, and financial platforms. In addition, it introduces key concepts such as social engineering and phishing, outlines how to secure digital and email accounts, and addresses other related topics.

Online Fraud and Forgery:
A Key Awareness Focus Topic

The National Cyber Security Agency recognises the scale and severity of growing cyber threats that currently affect individuals, institutions, and governments. Accordingly, the Agency has given particular attention to raising public awareness of these risks, notably including online fraud and forgery.

As part of the National Initiative for Digital Safety, the Agency has designated this topic as one of the core subjects featured in its training booklets.

The booklet titled Online Fraud and Forgery offers a clear and detailed explanation of the concept of digital forgery. It also defines and categorises types of online fraud and outlines practical guidance on how to protect against them. This includes verifying the source of email communications, avoiding the sharing of sensitive information, and using security software and regular system updates.

The Cyber Sanctuary:

An Engaging Learning Experience Through Realistic Fraud Scenarios

As part of the effort to diversify the awareness and training tools delivered to the target audience within the National Initiative for Digital Safety, the initiative's team has developed a set of interactive training games designed to support the National Cyber Security Agency's objectives in awareness, education, and training. Among these tools is the game The Cyber Sanctuary, created specifically to raise awareness among senior citizens about how to protect themselves from online fraud.

The Cyber Sanctuary aims to teach senior citizens how to safeguard their financial and banking accounts from fraud, while helping them recognise common scam attempts—such as suspicious messages or fake calls—and increasing their confidence in using digital applications and services safely.

The game uses playing cards that feature realistic fraud scenarios, such as a phone call pretending to be from a bank asking for account details, or a message from an unknown sender claiming a prize and requesting personal information. After choosing a response, the card is opened to reveal the outcome, along with an explanation of why the answer is correct or incorrect.

Field Visits:

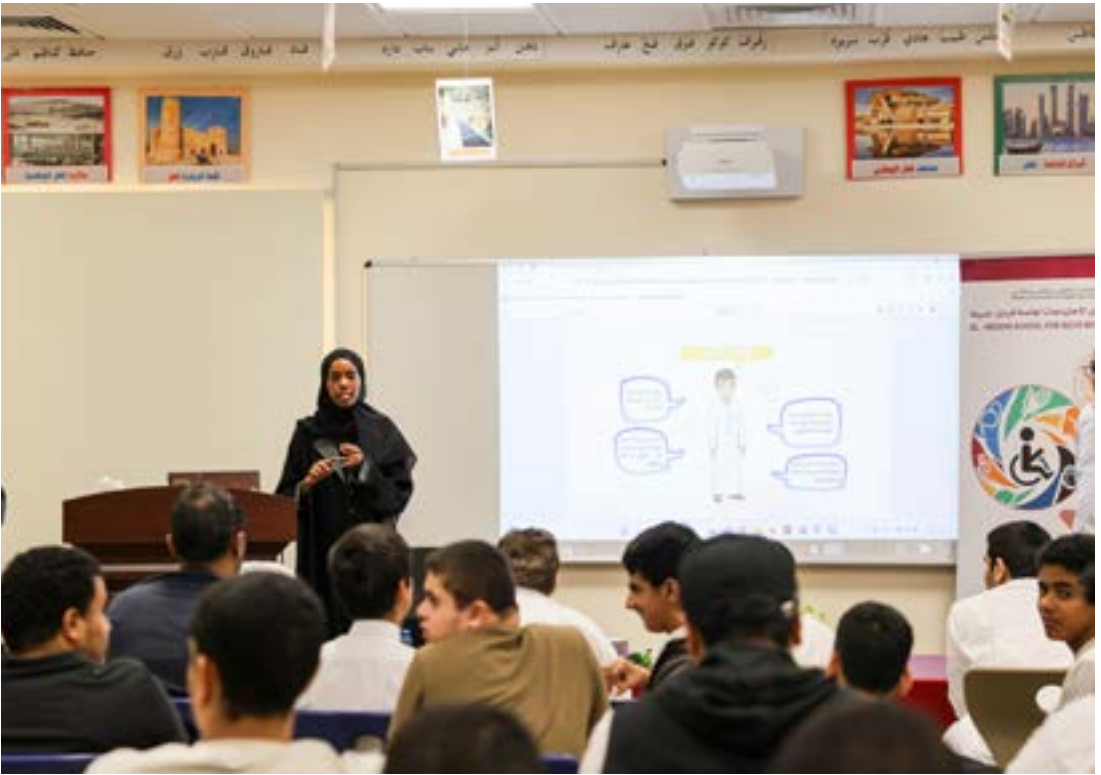
Highlights and Photos

As part of the National Initiative for Digital Safety, the National Cyber Security Agency conducted a series of field awareness workshops targeting diverse community segments. These sessions aimed to promote cybersecurity awareness and equip participants with practical guidance for safer digital behaviour. **Below are the highlights from the initial phase of these visits:**

Sunday, 27 April 2025 – Qatar Financial Centre (QFC), Doha

An awareness workshop titled “Cybersecurity Risks” was conducted for students, covering key principles of digital safety, personal data protection, securing smart devices and online accounts, responsible social media use, and methods for preventing various types of cybercrime.


مدرسة الهداية لذوي الاحتياجات الخاصة للبنين - السيلة
AL - HEDAYA SCHOOL FOR BOYS WITH SPECIAL NEEDS



Thursday, 8 May 2025 – Shafallah Center for Persons with Disabilities, Doha

A session titled “Identity Theft Online” introduced students to the concept and types of identity theft, reasons it occurs, its impact on internet users, preventive measures, and the appropriate steps to take when facing identity theft.

Thursday, 8 May 2025 – Dukhan English School, Dukhan

A cybersecurity awareness workshop titled “Cybersecurity Risks” focused on introducing students to major digital challenges, the consequences of unsafe internet practices, proper handling of personal and sensitive data, and essential safety measures when encountering cyber incidents.

Ehsan Centre for Empowerment and Elderly Care (Men›s Section), Doha

A session titled “Online Fraud and Forgery” was conducted, addressing the concept, types, and enablers of online fraud. It also covered personal data security, the importance of a digital footprint in preventing fraud, and practical safety tips.

Ehsan Centre for Empowerment and Elderly Care (Women›s Section), Doha

A similar workshop titled “Online Fraud and Forgery” was held for female participants, focusing on types and causes of digital fraud, reasons individuals fall victim to such crimes, and the role of personal data security and digital footprint awareness in prevention.


National Cyber Secur

Monday, 12 May 2025 – MIE-SPPU Institute of Higher Education (Pune University Doha Campus), Doha

A workshop titled "Mobile Applications and Privacy Protection" introduced students to the risks associated with mobile apps, types of data collected, reasons behind data collection, signs of malicious software on mobile devices, and how to minimise privacy breaches.

Tuesday, 13 May 2025 – Ministry of Labour, Doha

An awareness workshop titled "Unlicensed Software Downloads and Their Risks" was delivered, covering the types of software, software piracy, risks of using unlicensed programs, common viruses linked to such software, and effective protection strategies.

Tuesday, 13 May 2025 – Al-Hidaya School for Special Needs, Al Sakhama

A session titled "Identity Theft Online" focused on defining identity theft, its types and causes, its negative impact on internet users and their personal data, key prevention strategies, and response steps in the event of identity theft.


Mr.Abdullah khalil
(Cyber security trainer)
Mr. Saeed Mohammed
(Cybersecurity Specialist)


البرمجيات الخبيثة
Malware
الفيروسات
برمجيات الفدية
التجان الحاسوب
برمجيات التجسس


Mr.Abdullah khalil
(Cyber security trainer)
Mr. Saeed Mohammed
(Cybersecurity Specialist)

By the Numbers:

Week One of the National Initiative for Digital Safety

Total awareness

08 workshops conducted

02 for senior citizens

02 for persons with special educational needs

01 for expatriate workers

02 for school students

02 for university students

Awareness activities delivered in Week One

- Delivery of awareness content
- Presentation of visual awareness materials
- Presentation of training booklets
- Presentation of gifts

Total participants: **452**

Booklets presented: **452**

Gifts presented: **452**

Initial Field Visits of the National Initiative for Digital Safety:

Outcomes and Impressions

As part of the field visits conducted under the National Initiative for Digital Safety, electronic surveys were presented to participants in the awareness workshops held during the first week. The surveys aimed to assess the level of benefit gained from the awareness content and to gather participants› impressions of both the teacher's performance and the initiative.

Benefit from Awareness Content

91.9% of participants found the awareness content clear and easy to understand.

97.3% reported that they became aware of cyber risks and how to protect themselves.

91.9% rated the initiative as excellent.

Impressions of teachers' Performance

81.3% of participants believed that the teachers were able to deliver the content effectively.


البرمجيات الضارة


الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency
المبادرة الوطنية للسلامة الرقمية
Digital Safety National Initiative


الجرائم الإلكترونية
1
2
3


Cybershield:Cybersecurity Essentials for All


WORKSHOP
Cybershield:Cybersecurity Essentials for All