الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Monthly Newsletter

National Initiative for Digital Safety

In this issue

As part of its commitment to raising awareness across diverse segments of society:

The National Cyber Security Agency

continues to organise awareness-raising workshops under "the National Initiative for Digital Safety"

As part of its commitment to enhancing public awareness of cybersecurity concepts and digital safety standards and establishing a secure national digital space free from cyber threats, the National Cyber Security Agency continues to organise awareness-raising workshops under the National Initiative for Digital Safety. These workshops form part of an integrated awareness program comprising theoretical knowledge and practical training on the risks and threats individuals may encounter in their daily use of technology and when navigating cyberspace.

The Initiative aims to achieve several key national objectives. These include developing a well-structured national awareness framework for cybersecurity and digital safety to enhance knowledge across all segments of society; raising national standards of cybersecurity and digital safety; establishing a safe cyberspace for children, teenagers and young people; promoting a culture of cybersecurity and digital safety throughout society; enhancing safe access to the Internet; and addressing harmful behaviours and risks associated with the use of technology and the Internet.

Through the Initiative, the National Cyber Security Agency seeks to contribute to the achievement of Qatar National Vision 2030 by enhancing digital safety; developing cybersecurity talent among children, teenagers and young people; creating a supportive, knowledge-rich environment that supports the State's digital transformation; and providing added cybersecurity value to society. Collectively, these outcomes will contribute to enhancing the State of Qatar's standing on the Global Peace Index and other relevant national, regional and international indicators.

By the end of the sixth month, 39 awareness-raising workshops were delivered, including three for women and families, five for Senior Citizens, nine for expatriate workers, four for university students, three for people with special needs, eight for civil society organisations, two for the financial and banking sector, and five for the public and private sectors. In total, the workshops reached 26,753 participants.

Shared Digital Responsibility...
Enhancing Social Stability and Community Safety

Dalal Al-Aqeedi
Assistant Director of the Cybersecurity Policies and Strategies Department

In today's highly interconnected and rapidly changing world, we must take bolder, more decisive steps to establish cybersecurity as a societal priority indispensable to any state pursuing development and progress. Cybersecurity is no longer a luxury or a matter of prestige; it is an essential prerequisite for national progress and stability and for protecting national assets, particularly given that the economic cost of cyberattacks is projected to reach approximately US$10.5 trillion in 2025.

In practice, states that prioritise cybersecurity awareness are better positioned to advance economic development. A secure cyberspace enhances investor confidence, protects intellectual property and ensures the continuity of e-commerce and innovation. By contrast, states with limited cybersecurity awareness are exposed to mounting risks that can disrupt development or bring it to a standstill.

There is no doubt that establishing cybersecurity and achieving digital safety are shared societal responsibilities of state institutions and the public at large. State institutions are responsible for raising awareness of cybersecurity and digital threats, while the public is responsible for using technology safely and for playing an active role in digital protection rather than remaining passive targets.

In this context, the national initiatives launched by the National Cyber Security Agency play a key role in enhancing public awareness of digital safety. These range from the Educational Cybersecurity Curriculum for school students to the National Initiative for Digital Safety, which delivers awareness-raising workshops for senior citizens, employees in the public and private sectors, civil society organisations, women and families, and other segments of society. The Agency's comprehensive approach to implementing the Initiative is essential to the development of a digitally aware and responsible society that can respond swiftly to cyber incidents and manage them safely, thereby promoting prosperity and social well-being in a rapidly evolving cyberspace. It is therefore not only a matter of security but also of sovereignty, prosperity and social harmony.

Over 26,000 benefited from awareness-raising content:

“The National Initiative for Digital Safety ”… Achieves Quality and Quantity Success

The National Cyber Security Agency, under the National Initiative for Digital Safety, has delivered several quantitative and qualitative achievements. Qualitatively, the initiative has brought about clear, observable changes in behaviours and perceptions related to digital safety across the target groups, and has increased overall public awareness of related topics.

Feedback obtained from the questionnaires distributed to participants at the conclusion of the awareness workshops revealed that around 94.5% found the content clear and accessible, while 93.2% reported a better grasp of cyber risks and how to prevent them. In addition, 93.6% rated the initiative as excellent.

Quantitatively, the initiative reached over 26,000 beneficiaries through tailored workshops for various target groups. It successfully encouraged direct engagement with the content, with about 39 workshops organised across all categories. Over 26,000 training booklets were distributed, further reinforcing the awareness content among the general public.

These qualitative and quantitative achievements clearly reflect the initiative’s role in creating a secure and positive digital environment that supports the principles and foundations of digital citizenship and sustainable community development.

Internet Fraud
A Key Awareness Focus for Senior Citizens

One of the most significant digital threats facing internet users is online fraud and cyber forgery. Internet fraud involves deceptive practices carried out via the internet, often through chat rooms, email, forums, or websites. The primary goal is to deceive users and clients by stealing money, personal information, and other sensitive data.

The National Initiative for Digital Safety is keen to address these pressing issues through a dedicated awareness portfolios developed specifically for Senior Citizens. It covers a range of issues related to cyber forgery, including:

- Cyber Fraud and Forgery
- Types and forms of online fraud
- Vulnerabilities that enable online fraud
- Digital footprints and their link to online fraud
- Protective measures against online fraud
- Official authorities to contact when facing cyber fraud

Artificial Intelligence
A High-Risk Cyberattack Weapon

The National Cyber Security Agency closely monitors the international digital landscape, tracking rapid and unprecedented technological advancements alongside a notable rise in cyber threats targeting individuals, organisations, and communities. Of particular concern is the significant progress in Artificial Intelligence (AI) and its advanced techniques, which have become a major cybersecurity threat. AI is increasingly used to enhance the scale and sophistication of cyberattacks against individuals and businesses.

AI technologies and tools have become a dangerous offensive weapon in the digital space. For example, they are used to craft intelligent phishing messages, leveraging text-generation models like GPT to create highly convincing emails. AI also powers adaptive malware that bypasses traditional security software, exploits vulnerabilities, and generates deepfake images and videos to impersonate influential figures for fraud or disinformation campaigns.

Recognising these risks, the Agency has integrated AI into the National Initiative for Digital Safety. This ensures targeted groups receive the necessary knowledge and training to navigate this fast-evolving field, understand its close ties to cyber threats, and learn how AI can be used defensively to prevent, repel, or at least mitigate the impact of digital attacks once occurred.

Child Digital Safety

A National Priority for Protecting Children Online

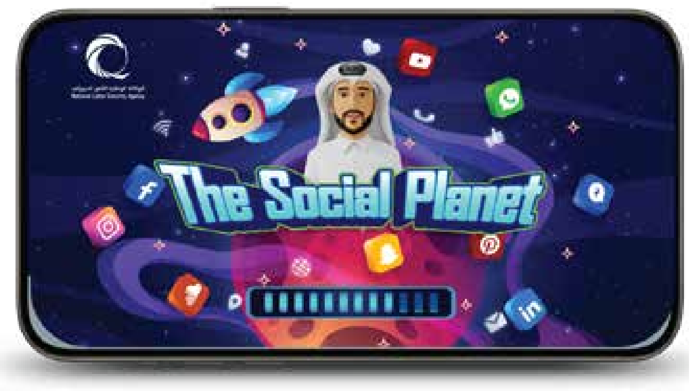
The National Initiative for Digital Safety is a flagship project of Qatar's National Cyber Security Agency, aimed at safeguarding the country's cybersecurity. A key goal of this initiative is to enhance digital safety indicators for children.

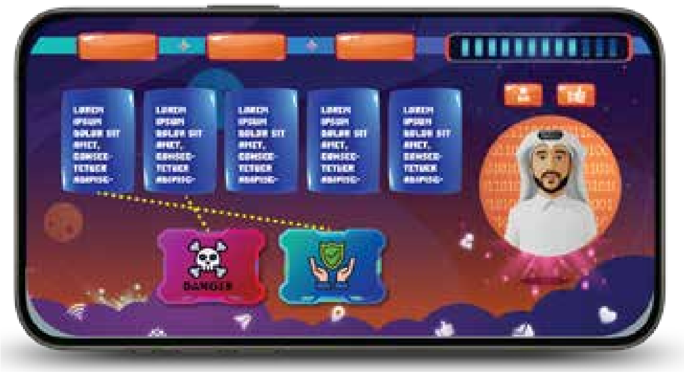
The Agency's focus on children and adolescents aligns with Qatar's broader efforts to protect young people in the digital space. Qatar is a regional leader in promoting child cybersecurity, having taken significant steps such as establishing the Cybercrime Combating Center, strengthening internet crime legislation, and issuing recommendations to develop digital laws that ban harmful content and criminalise online violence against children.

The Agency has launched several important initiatives, including the Cybersecurity Educational Curriculum project. This targets all public and private schools, grade levels, and parallel education students, providing specialised content on cybersecurity and digital safety. Another initiative is the "Cyber Eco" School Visits project, which engages three key educational stakeholders: students, teachers, and parents through training workshops on digital safety and secure internet use.

Additionally, the initiative targets women and families, with a primary focus on children and adolescents. It offers diverse training materials (print and visual) on cybersecurity risks and family digital safety, alongside entertaining content such as printed and electronic games. These resources enhance theoretical knowledge, hands-on training, and digital skills in an engaging and enjoyable mode of learning.

"The Social Planet": A Gamified App Blending Fun with Cyber Awareness





The National Cyber Security Agency recognises that electronic games are an effective awareness tool for various target groups of the National Initiative for Digital Safety. Games deliver knowledge through interaction, excitement, and sustained engagement, while tailoring content to suit the age and functional characteristics of each target group. This approach enhances learning outcomes and promotes understanding of cybersecurity and digital safety concepts.

One such game is "The Social Planet", designed for university students. The game features a planet representing the most popular social media platforms among this segment of society, with icons symbolising platforms like (Facebook, X, Instagram, Snapchat). Players navigate between these icons, answering questions related to each platform to earn points and progress to more challenging levels.

The game aims to educate students on key cybersecurity principles and digital safety practices in their daily activities. It provides highly specialised cybersecurity information relevant to university students, explains basic cybersecurity terms and concepts in simple, accessible ways. This game combines learning with suspense and motivation to win. It also offers entertainment through progressively challenging puzzles.

Cybersecurity Awareness Portal ...
Direct Public Engagement

The National Initiative for Digital Safety includes a range of activities addressing the digital knowledge needs of target community groups. Recognising the importance of direct engagement, the Agency launched the Mobile Cybersecurity Awareness Portal, a pioneering initiative at the national and regional levels. This portal is deployed in public spaces frequently visited by the general public.

The portal features an AI-powered chatbot that simulates human conversations, interacts with visitors, answers their questions, and provides additional services such as digital behaviour analysis and smart device security testing.

Some portal activities make use of advanced digital technologies, including 3D technology, which immerses visitors in interactive virtual environment that responds naturally to their actions, mimicking real-life scenarios. This is achieved using head-mounted displays that transport users into digital experiences where they engage with characters and situations related to technology and cybersecurity.

As part of this initiative, the Agency organised a back-to-school cybersecurity awareness event at Vendôme Mall from 27 August 2025 to 29 August 2025. The event witnessed significant participation, particularly from children who enthusiastically interacted with virtual reality headsets and the chatbot robot.

Another event was held at The West Walk from 16 September 2025 to 19 September 2025, where awareness tools, including the interactive robot, touchscreens, and electronic games, attracted a large number of visitors and generated high levels of engagement.

Highlights from Awareness Workshops

Sudanese Women's Association

رابطة المـرأة السودانية (ســوا) - قـطـر
udanese Women Association (SWA) - QATAR

On Saturday, 5 July 2025, the Agency held a workshop at the Sudanese Women's Association titled "Family Digital Safety and Cybersecurity Risks". Attendees learned about digital safety principles, secure and positive internet use, data breach tactics, common identity theft methods, and the family's role in protecting children online.

Ministry of Labour and Workers' Support Fund

وزارة العمل
Ministry of Labour
State of Qatar • دولة قطر

On Tuesday, 8 July 2025, a workshop was conducted at the Ministry of Labour and Workers' Support Fund on "Unlicensed Software Downloads and Associated Harm". Participants were educated about the risks of pirating software and downloading malicious programs from untrusted sources. The session emphasised the importance of using official sources for downloading software and applications.

Aman Center

On Sunday,10 August 2025, the Agency held a workshop at Aman Center on "Family Digital Safety". The session covered concepts of cybersecurity and digital safety for all family members, principles of safe and positive internet browsing and technology use, as well as the family's role in protecting children in the digital space.

Institute for Graduate Studies

On Wednesday, 27 August 2025, a workshop was organised at the Institute for Graduate Studies on "Mobile Apps and Privacy Protection". Students were introduced to concepts related to smartphone apps, common risks, types of user that apps collect surreptitiously and red flags of malicious software. They also were educated on countermeasures when privacy is threatened by mobile applications.

Social Insurance Authority

الهيئة العامة للتقاعد والتأمينات الاجتماعية
General Retirement & Social Insurance Authority

On Wednesday, 3 September 2025, the Agency held a workshop at the General Retirement and Social Insurance Authority titled "Online Fraud and Forgery". The session focused on Senior Citizens, covering concepts of common types of online fraud, vulnerabilities exploited by attackers, the importance of personal data security, and the role of digital footprints in preventing cybercrimes.

Qatar Press Center

المركز القطري للصحافة
QATAR PRESS CENTER

From Sunday to Tuesday, 7–9 September 2025, a workshop was conducted at the Qatar Press Center under titled "Protecting Media Data". Aimed at journalists and media professionals, it addressed safe email and social media practices, digital application security, and strategies to protect organisations from cyberattacks and breaches.

Qatar Charity

On Monday, 8 September 2025, the National Cyber Security Agency (Qatar) organised a workshop at Qatar Charity titled "Protection of Confidential Data". The session educated attendees on types of confidential professional data that should not be accessed externally, data breach tactics, exploitation in digital attacks targeting data and organisational stability, and preventive measures.

Al Rayan Bank

بـنـك الريـــان
ALRAYAN BANK

On Tuesday, 9 September 2025, a workshop was held for Al Rayan Bank employees on "Digital Safety in Financial and Banking Institutions". Topics included digital safety concepts in finance, protecting banking transactions, common cyber challenges in the sector, exploitable vulnerabilities manipulated to carry out such attacks, and employees' roles in preventing financial cyber incidents and help establish digital safety in their workplace.

Ministry of Transport

From Sunday to Thursday, 14–18 September 2025, the Agency conducted a workshop at the Ministry of Transport titled "Digital Safety". Participants were educated on cybersecurity principles, safe internet and technology use, and strategies to avoid cyber incidents and attacks.

Ministry of Social Development

وزارة التنمية الاجتماعية والأسرة
Ministry of Social Development and Family

On Wednesday, 17 September 2025, a workshop was held at the Ministry of Social Development and Family on "Protection of Confidential Data". It covered the importance of digital data, data classification, common data theft methods, and prevention strategies.

Ehsan Centre

On Sunday, 28 September 2025, the National Cyber Security Agency conducted an awareness workshop at Ehsan Centre on "Online Forgery and Fraud". The workshop introduced Senior Women to the concept of online fraud, the most prevalent types and the common mistakes made by internet users that can lead to digital fraud attacks. The workshop aimed at raising participants' awareness of the importance of protecting personal data security.

Qatar University

جامعة قطر
QATAR UNIVERSITY

On Tuesday, 30 September 2025, the National Cyber Security Agency held an awareness workshop at Qatar University titled "Mobile Applications and Privacy Protection". The workshop educated participating students on key concepts related to smartphones, the most common vulnerabilities in their applications, and what user data collected by these malicious apps without users' knowledge. Students also learnt how to avoid data theft and privacy thr eats when using smartphones.

Thursday, 10 Rabi al-Thani 1447 AH – 2 October 2025 CE

Hamad Medical Corporation

On Thursday, 2 October 2025, the National Cyber Security Agency held an awareness workshop at Hamad Medical Corporation titled "Protecting Confidential Information". The workshop covered the importance of business-related information and helped participants understand which types of information can be shared with external stakeholders and which confidential data should remain restricted to internal staff only. Participants also learned about the principles of protecting sensitive information from cyber theft, which is often carried out for purposes of blackmail or extortion.

The Third Month of the Awareness-Raising Workshops

Activities conducted in the sixth month

- Presentation of awareness content
- Presentation of visual awareness content
- Distribution of training booklets

Sixth Month of Awareness Workshops .... Outcomes and Impressions

As part of the awareness workshops conducted under the National Initiative for Digital Safety, electronic surveys were distributed to participants during the sixth month to evaluate the benefits of the awareness content and gather feedback on trainers' performance and the initiative overall.

Benefits of Awareness Content

94.5%

of participants found the content clear and accessible.

93.2%

of participants are aware of cyber risks and countermeasures.

93.6%

rated the initiative as excellent.

Impressions of Trainers' Performance

82.9% confirmed that the trainers effectively delivered the awareness content.

Targeted Groups