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

Monday, 5 Muharram 1447 AH, 30 June 2025 CE

Towards a Safer Digital Space Free of Threats: National Cyber Security Agency Rolls Out Awareness Workshops Under the “NATIONAL INITIATIVE FOR DIGITAL SAFETY”

As part of its ongoing efforts to lay the foundations of public awareness nationwide regarding cybersecurity principles, digital safety controls, and means to have access to a safe national digital space free of threats, the National Cyber Security Agency organizes awareness workshops under the "National Digital Safety Initiative". These workshops are directed to diverse society segments in Qatar, including senior citizens, women and family, government and private sector employees, expatriate workers, financial and banking institutions' staff, and others. These awareness-raising workshops provide trainings and knowledge support to enable them to have a safe and threat-free experience of using the internet and its applications.

The initiative is structured around a whole host of activities and public awareness events that seek to strengthen national cyberspace resilience as a key foundation for supporting the state's advancement across all vital sectors, while promoting a culture of digital safety on multiple fronts, i.e., socially and governmentally in a way that reinforces the government's efforts to achieve the National Vision 2030, the Cyber Security Strategy 2024-2030, and the Third National Development Strategy 2024-2030.

The initiative strives to achieve Qatar Vision 2030 through its contribution to the first pillar (Human Development) by enhancing social awareness of digital safety concept, empower individuals to interact safely with technology and its tools and applications, which in turn directly contributes to boosting society's security against cyber threats, breaches, and electronic crimes targeting individuals. The initiative works directly to protect community members against the effects of cybercrime by building and enhancing cyber awareness.

By the end of the third month, 20 workshops will have been conducted, with awareness content delivered to 1,105 participants and 1,105 training booklets distributed. During the third month alone, 7 workshops were held: one for civil society, one for women and families, one for the elderly, and four for expatriate employees. The awareness content reached 529 participants, with 529 training booklets handed out accordingly.

Digital Safety Initiative
National Project Requires Everyone's Support to Succeed

The National Cyber Security Agency is always keen to align its community initiatives with the national development efforts in technology and cybersecurity, being a key approach to sustain their positive impact for decades to come.

The Agency staff views the "National Initiative for Digital Safety " as a national cause that requires everyone's involvement including institutions, authorities, and all members of society. The goal is ambitious: achieving advanced societal awareness in cybersecurity and digital safety amid the challenges posed by rapid changes in our digital world.

The initiative draws directly from Qatar Vision 2030 and the National Cyber Security Strategy, which guide all development activities across the state. It takes a comprehensive approach, training different segments of society to handle modern technology safely and effectively, improving digital education for students and the public, and fostering innovation in the digital field. The initiative enables all community members to interact creatively with technology—a core principle of Qatar Vision 2030 and the Cyber Security Strategy.

Dalal Al-Aqeedi

Director of the National Cyber Excellence Department

This national vision will drive community cyber awareness efforts and strengthen Qatar's standing on key international rankings, including the Global Cybersecurity Index, E-Participation Index, ICT Development Index, and Digital Infrastructure Readiness Index.

Family Digital Safety...

A Key Pillar for Digital Citizenship

Amidst rapid technological developments and their integration into all aspects of modern life, the pace of cyber threats against individuals and various business institutions is escalating. At the individual level, these threats extend to reach family members of varying ages and cultural and technical backgrounds. Such threats range from ransomware attacks and social engineering to malware, online fraud, and data breaches.

The "National Initiative for Digital Safety " has recognised the severity of these threats that jeopardise digital family security and stability. To achieve its objectives of raising cybersecurity awareness levels among the broader local society and maximising benefits from technology without compromising digital safety, it's imperative for all family members to adopt precautionary measures including familiarisation with digital safety basics and principles, alongside protocols for safe and responsible use of the internet, applications, and programmes. This represents the essence of digital citizenship.

Family digital safety constitutes one of the principal awareness packages delivered to the women and family segment, covering the following areas:

- Personal data breaches
- Common methods used in data breaches
  - Phishing
  - Brute force attacks
  - Malware
- Data breaches and cybercrimes against women
- Family digital safety
- Women's digital safety
- Family's role in protecting children online
- Steps to follow when identity theft occurs
- General digital safety guidance

Monday, 5 Muharram 1447 AH, 30 June 2025 CE

National Initiative for Digital Safety...

A Robust Research-Based Methodology

In line with the National Cyber Security Agency's commitment to bolster the scientific approach in implementing the National Initiative for Digital Safety and keeping pace with objective research-based principles, the Agency has focused on staying attuned to the working practices of leading international research institutions in cybersecurity and digital safety. This enables identification of the key operational foundations of these centres and decide the best way to make use of their experience in enhancing the initiative's chances of success and ultimately achieving its vision and mission.

The study has examined outputs and findings of those international research centres and institutions related to cybersecurity and digital safety and was able to identify the latest international cyber research trends and prominent cyber research issues of interest to these centres. Moreover, global high priority themes were selected to be included within the awareness content to be delivered under the National Initiative for Digital Safety.

The study focused on analysing early recovery methodologies from cyber attacks, suitable awareness content for dealing with psychological impacts resulting from cyber attacks at the individual level, and development of a national strategy for early recovery from cyber incidents across multiple sectors: individuals, children, government and private institutions, and financial and banking institutions.

Monday, 5 Muharram 1447 AH, 30 June 2025 CE

Cyber Awareness Portal...
Simulating Human Conversations

In keeping with the National Cyber Security Agency's commitment to engaging closely with the local public across various venues throughout the state, the Agency continues to organise Mobile Cyber Awareness Portal events as part of the "National Initiative for Digital Safety " activities. This pioneering experience at both national and regional levels features a plethora of interactive activities that appeal to different age groups.

The portal features an AI-powered chatbot that simulates human conversation to interact with visitors, answer their queries, and analyse their digital behaviour through a series of questions concerning their behaviour of internet browsing, types of passwords, and privacy practices. This service operates by directing questions to the robot, which responds and determines whether their digital behaviour is appropriate or not.

The portal also features digital technology with a three-dimensional environment that surrounds users and responds naturally to their actions through head-mounted displays. Through this technology, a 3D video introducing basic concepts of digital safety in a customised mode to appeal to the needs of each segment. The video features two sets of icons, the first of which represents digital safety tools such as shields, eagles, and locks, and the other one depicts cyber threats such as spiders and snakes.

The Power of Play... Use Games to Teach Cybersecurity Awareness

Games are a proven, powerful approach to education, awareness-raising, and training since games are inherently interactive and effective achieving intended outcomes through a more enjoyable learning experience. Recognising this reality, the "National Initiative for Digital Safety " has been careful to provide a collection of printed and digital cyber games tailored to each type of target audience. The overarching objective of these games is to enhance public awareness of cybersecurity concepts and digital safety basics through hands-on gamification experience.

The printed and electronic games have been designed to suit the age-related, psychological, social, and professional characteristics of target demographics. For example, there is the "Cyber Woman" game for women, which simulates the online shopping experience. Virtual female shoppers face various real-world challenges such as tempting offers, payment methods, personal data protection, and other problems they might encounter during shopping errands.

There is also the "Cyber Lighthouse" game aimed at senior citizens, which is dedicated to train the elderly segment on ways to protect their financial and banking accounts from online fraud crimes. The game also helps them adopt safe behaviors if they experienced fraud. In addition, it aims to boost their trust in using digital applications and services safely. The game includes various questions about different scenarios, such as receiving fraud WhatsApp messages requesting personal information or getting calls claiming to be from their respective banks requesting data updates.

Cybersecurity... Promising Fields and Pressing Priorities

Cybersecurity is closely tied to rapid technological and scientific advancement in the digital ecosystem, and is significantly influenced by these developments. In response, the field has expanded to encompass promising sub-disciplines that garner growing international attention from various stakeholders—individuals, leaders and decision-makers, entrepreneurs and business professionals. These areas include cloud security and artificial intelligence.

Cloud security refers to a set of procedures and technologies designed to protect data, applications, and infrastructure in cloud environments. It is considered a cornerstone of cybersecurity as the core mission of this field is to combat threats targeting cloud computing resources such as data theft, unauthorised access, or cyber attacks, ensuring integrity, confidentiality and availability of sensitive information.

Artificial intelligence has become a cornerstone of cybersecurity and an important field within it. It can be leveraged across several key areas, particularly in combating cyber attacks. The agile nature of AI and its exceptional ability to process vast amounts of data in record time, enabled it to identify and deal with potential digital vulnerabilities before they are even discovered by attackers. Moreover, AI technologies can be utilised to support recovery indicators following cyber attacks.

Although cyber attackers have already exploited artificial intelligence technologies to develop cyber attacks for increased success rates by identifying digital vulnerabilities quickly. It is also used for deepfakes and creation of phishing messages that are difficult to detect. The silver lining is that this cutting-edge technology can equally be harnessed to develop swift and robust countermeasures against these threats, as well as adoption of preventive and remedial strategies and policies for immediate response to these sophisticated cyber attack patterns.

Social Engineering...
Staying Alert to Email Communications

As email communication has become ubiquitous in both professional and personal contexts, its widespread use across various levels makes it an attractive tool for executing cyber attacks, being one of the most commonly exploited channels for social engineering. These attacks rely on manipulating users emotions and gaining their trust to trick them into sharing sensitive personal information or clicking malicious links.

Responding to this pressing issue, the "National Initiative for Digital Safety" dedicates a considerable portion of its awareness-raising content to educating target audiences on how to stay alert when using email, whether for personal purposes, work, or friendly communication. They are also familiarised with common fraud methods and cyber attack execution via email, such as unsolicited email messages or those containing unknownattachments.Thesecancarry malicious software that infiltrates user accounts or devices, breaching accounts and stealing personal and business-related data.

The awareness content emphasises the importance of avoiding clicks on suspicious links, even those that appear to be from known sources. Rather, they should verify them first, and delete messages proven to be from unknown, untrusted sources.

MESSCAFE
Heat Stress, Workplace Safety & Cybersecurity Awareness Session
وزارة العمل
Ministry of Labour

Workplace Cyber Attacks...

Organised Threats and Devastating Losses

Employees across government, private sector, financial services, banking, and civil society organisations represent a substantial portion of the local community. For this reason, the "National Initiative for Digital Safety" targets these groups with awareness campaigns about the various cyber risks they face in their working environments. This involves familiarising them with the concept of professional cyber threats and identifying the most prevalent types of attacks that target digital systems and sensitive data within companies and business institutions.

Cyber risks in workplace settings are diverse and extending to multiple threat levels. These can be categorised into insider threats, which occur when current or former employees exploit their access privileges to compromise company data or disrupt operations; advanced persistent threats (APTs), which are sophisticated, long-term organised attacks aimed at stealing sensitive information or conducting espionage on systems, typically executed by highly skilled technical groups; cloud security breaches targeting company data stored on cloud platforms; and various other attack vectors.

The initiative addresses these risks through theoretical awareness content, visual materials, and interactive electronic games that identify different attack types, such as system infiltration attempts, information theft, and malware distribution—all of which can lead to work disruption, and substantial financial and reputational losses. Additionally, emphasis is placed on crucial security measures recommended for preventing these attacks or minimising their adverse consequences should they occur. On top of this are regular system update, strong passwords and changing them frequently, and raising awareness about phishing scams to safeguard data against cyber attacks.

Highlights from Awareness Workshops

Ministry of Labour

The National Cyber Security Agency organised an awareness workshop at the Ministry of Labour on Saturday, 31st May 2025, titled "Unlicensed Software Downloads and Their Risks". Participants were briefed on various computer programmes and their types, the concept of software piracy, threats associated with downloading unlicensed software, and the most common types of malicious viruses linked to unlicensed programmes, along with prevention methods.

The National Cyber Security Agency organised an awareness workshop at the Ministry of Labour on Saturday, 31st May 2025, titled “Unlicensed Software Downloads and Their Risks”. Participants were briefed on importance of downloading licensed programmes from trusted sources and consequences of not following safety rules and how this could be detrimental to smart devices.

Ministry of Labour

وزارة العمل
Ministry of Labour
State of Qatar • دولة قطر

On Friday, 6th June 2025, the National Cyber Security Agency held another awareness workshop at the Ministry of Labour addressing "Unlicensed Software Downloads and Their Risks". The session covered concepts relating to computer programmes and smartphone applications, emphasising the importance of downloading trusted software from official sources such as established technology companies' digital stores (Google Play Store/ App Store), and the negative consequences that may arise from downloading unofficial programmes, including device and account breaches through malicious viruses.

Center for Empowerment and Care of the Elderly (Ehsan)

The National Cyber Security Agency conducted an awareness workshop on Wednesday, 18th June 2025, at Center for Empowerment and Care of the Elderly (Ehsan) entitled "Online Fraud and Deception". The session focused on raising awareness amongst senior citizens about the concept of online fraud and its most common types, vulnerabilities that facilitate electronic fraud operations, and introduced participants to the importance of personal data security and the role of digital footprints in preventing online fraud crimes.

Ministry of Labour

On Friday, 20th June 2025, the National Cyber Security Agency organised a workshop at the Ministry of Labour on "Unlicensed Software Downloads and Their Risks", where participants learned about the dangers of pirating computer and smart device software using malicious programmes downloaded from unofficial applications and unreliable sources. They were educated on the necessity of turning to official sources when downloading electronic programmes and applications.

Sudanese Women’s Association

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

The National Cyber Security Agency held an awareness workshop at the Sudanese Women's Association on Saturday, 21st June 2025, entitled "Family Digital Safety". Participants were educated on digital safety principles and the positive and safe use of the internet and technological applications, introduced to personal data breaches and common methods used in such breaches, and informed about the family's role in protecting children online.

Qatar Foundation for Social Work

قطر للعمل الإجتماعي
Qatar Social Work

The National Cyber Security Agency conducted an awareness workshop on Tuesday, 24 June 2025, at the Qatar Foundation for Social Work, entitled "Protecting Confidential Data". Participants learned about different types of professional data classified as “confidential and not to be accessed”, how data breaches occur and are exploited for cyber attacks, and effective prevention strategies.

The Third Month of the Awareness-Raising Workshops

Activities conducted in the third month

- Presentation of awareness content
- Presentation of Visual Awareness Content
- Distribution of Training Booklets

The Third Month of Awareness-Raising Workshops....

Outcomes and Impressions

As part of the awareness-raising workshops conducted under the National Initiative for Digital Safety, participants completed electronic surveys to evaluate workshops held during the third month to assess the programme's effectiveness. The surveys assessed how much participants benefited from the content and gathered feedback on trainer performance and the initiative overall.

Engagement with the Awareness-Raising Content:

93.1 %

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

95.4 %

of participants demonstrated genuine understanding of cyber risks and appropriate prevention measures.

91.7 %

of participants rated the initiative as outstanding.

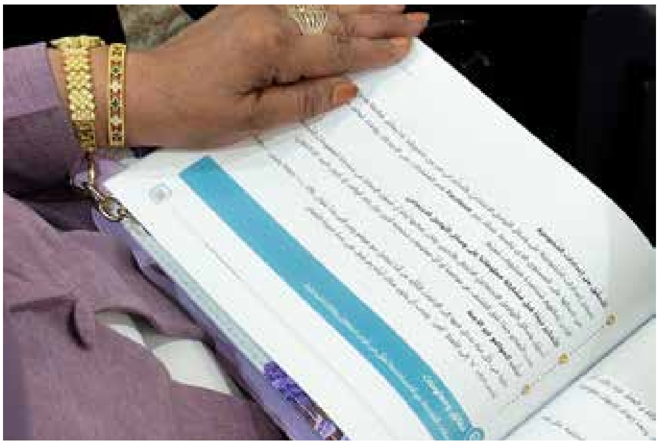
Trainer Effectiveness

83.5 %

of participants considering the trainers effective in presenting the awareness content

MESSCAFE
Workplace Safety & Cyberse

MESSCAFE



MESSCAFE

MESSCAFE