الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# Weekly Newsletter

## National Initiative for Digital Safety

## In this issue

With the objective of establishing a well-defined national framework for raising awareness of the principles and foundations of digital safety,

# The National Cyber Security Agency continues to deliver awareness-raising workshops under the National Initiative for Digital Safety.

As part of The National Cyber Security Agency's dedication to establishing a secure and effective national digital space, and to promoting a culture of digital citizenship and responsible internet use, the Agency continues to deliver awareness workshops under the National Initiative for Digital Safety. These workshops focus on education, awareness, and capacity-building in the fields of cybersecurity and digital safety, targeting various societal segments across the state.

The National Initiative for Digital Safety also seeks to achieve a sustainable qualitative improvement in public awareness of digital safety concepts and to develop a well-structured national framework for cybersecurity awareness. This objective is implemented through a series of activities and awareness-raising workshops informed by the findings of scientific studies and research conducted by the agency, ensuring that the initiative remains aligned with the latest internationally recognised methodologies and practices in cybersecurity awareness.

During the three-year duration of the initiative, awareness-raising workshops will be delivered to various segments of society, including employees in both the public and private sectors, expatriate workers, school and university students, staff of financial and banking institutions, and others. These awareness-raising workshops will support the long-term positive impact the agency aims to achieve.

To support the strategic direction of the initiative and ensure the continued impact and positive results at the local community level, the initiative was planned to contribute to the achievement of the Qatar National Vision 2030. This is done by raising public awareness of digital safety, improving the ability to use technology, its tools, and applications securely, and enhancing community security through the early prevention of cyber threats, breaches, and cybercrime. The initiative also supports the country's digital transformation efforts by contributing to the quality and security of the national technological environment. The National Initiative for Digital Safety is a direct contribution to both government and public efforts to achieve Vision 2030.

By the end of the second week of the awareness-raising workshops, 10 workshops had been conducted, and awareness content was delivered to 576 participants. In total, 576 training booklets were distributed.

During the second week alone, three workshops were held: one for individuals with special needs, one for employees in the financial and banking sector, and one for university students. A total of 124 participants received awareness content, and 124 training booklets were distributed.

# The Initiative: An Effective Tool for Strengthening Digital Trust and Building National Capabilities

The National Cyber Security Agency carries significant national responsibilities. These include protecting and regulating the national cyberspace, safeguarding the vital interests of the state, its institutions, and its people, and defending against the growing global digital threats. The Agency also continuously assesses the national cybersecurity situation, in coordination with other relevant entities, to proactively identify risks and respond using efficient and effective methods that deliver long-term positive outcomes.

As the main platform for the Agency's community awareness efforts, the National Initiative for Digital Safety is designed to help achieve these objectives. It focuses on improving digital safety indicators among various social groups, raising awareness of the main cyber risks and threats linked to the use of cyberspace, increasing their readiness to respond safely and early to these threats, and reducing the impact of such incidents while helping to prevent them from happening again. Like all countries, Qatar faces these current challenges, which are now a key part of the modern global digital environment.

**Dalal Al-Aqeedi**

Director of the National Cyber Excellence Department

Through the initiative, the Agency not only raises public awareness of cybersecurity but also supports and develops national capabilities in this field. It encourages innovation and creativity among children, young people, and youth-core target groups of the initiative-by providing them with innovative tools for education, awareness, and training based on the latest international standards and practices in cybersecurity. The initiative helps them use technology safely and effectively, building trust in digital interactions and expanding opportunities for cyber innovation and creativity. These efforts support one of the pillars of Qatar National Vision 2030, which the initiative contributes to through its various activities.

# Digital Safety Trends...

# and Awareness Needs Analysis

From the earliest stages of planning the National Initiative for Digital Safety, The National Cyber Security Agency has been committed to ensuring that the initiative adopts a comprehensive strategic approach at both the state and societal levels. Accordingly, the theoretical and training content of the initiative has been designed to address a broad and diverse range of social groups.

To ensure the success of the initiative in achieving its objectives among the target audience, The National Cyber Security Agency placed particular emphasis on analysing the cybersecurity knowledge levels across the various groups, and identifying the specific awareness and training needs for each. Accordingly, a comprehensive analysis of societal trends related to cybersecurity was conducted, along with an assessment of the actual state of digital safety indicators across various levels.

The analysis produced accurate and valuable data that supported the planning of the initiative's activities. This included: the percentage of internet and social media use among children and young people in the state; the percentage of awareness among this group of the risks associated with account breaches; the percentage of excessive internet use among children and young people; the percentage of their accounts exposed to cyberattacks; the percentage of parental awareness of digital risks facing children and young people; and the extent to which families are able to guide and support their children in dealing with cybersecurity risks.

# The Digital Safety Guide..

# A Key Element of Awareness-Raising

As technology becomes more integrated into daily life, a range of modern concepts has emerged that are closely tied to cybersecurity, whether related to the tools used, the emerging threats, or the core elements of cybersecurity itself. A clear understanding of these concepts has become a critical necessity for ensuring digital safety when using the Internet or current technological tools.

The National Cyber Security Agency focused on including these concepts and emphasising their importance as a main awareness focus of the National Initiative for Digital Safety. The Digital Safety Guide covers key modern cybersecurity concepts such as phishing, social engineering, privilege escalation, and ethical and unethical hacking. In parallel, electronic game applications address other advanced concepts, including password security, digital data, social media threats, the General Data Protection Regulation, financial cyberattacks, and workplace security elements, presented in engaging formats.

The awareness videos cover more specialised concepts, such as the principles of operational technology security, cloud computing and its uses, the link between hacking and smart cities, the difference between digital currencies and cryptocurrencies, and the concept of malicious software and its types, including social bots.

Among the more common modern concepts addressed in the initiative's content is ethical hacking. The material explores its definition and significance, the types of ethical hackers, and the relationship between ethical hacking and cyberattacks. It also covers the concept of digital currencies, the factors behind their emergence, the reasons they pose risks, and the related cyber threats.


# Senior Citizens and...

## Promoting Trust in the Safe Use of Technology

Qatar has a diverse social structure and a near-total Internet usage rate of 100%. This diversity results in considerable variation in how different groups engage with technology. As a result, during the planning of the initiative, The National Cyber Security Agency focused on addressing each social group through activities and events specifically designed to meet its cybersecurity awareness needs.

Senior citizens are one of the main groups targeted by the National Initiative for Digital Safety. As their use of the Internet and digital services continues to grow, it becomes increasingly important to raise their awareness about protecting personal data and information, and to educate them on maintaining privacy online. This includes using strong passwords and avoiding the sharing of sensitive information.

The initiative's activities also raise awareness among senior citizens about common types of online fraud, such as fake emails, scam phone calls, and suspicious links. All these efforts support the main objective: to strengthen their confidence in using technology safely and effectively.

# Online Identity Theft as a Focus of the Initiative

With the rapid development of technology and the widespread use of the Internet in all areas of life, digital threats now affect all segments of society. This increases the importance of ongoing efforts to raise public awareness of digital safety and cybersecurity as a way to reduce these threats.

As part of the efforts of The National Cyber Security Agency and within the National Initiative for Digital Safety, a booklet titled Online Identity Theft was developed for individuals with special needs. The booklet explains what identity theft is, its causes and effects, and provides general advice and guidance on digital safety.

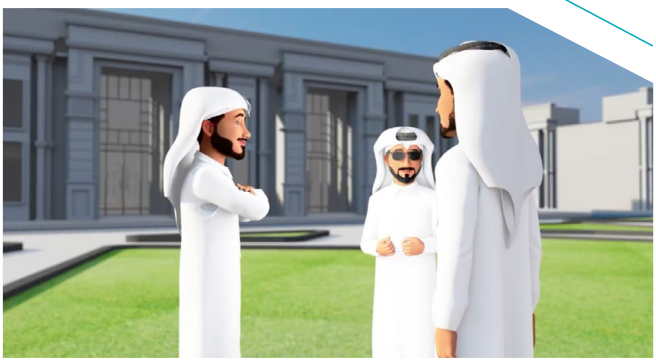
Online identity theft is one of the most common types of cybercrime. It continues to grow as technology advances and reliance on the Internet increases. This crime does not target a specific group; anyone can be affected, regardless of age, social background, education level, or technical knowledge. Offenders use social engineering techniques-advanced methods designed to deceive individuals by manipulating emotions such as excitement, fear, or the desire to win. This leads people to make unwise decisions, such as giving away personal or financial information without fully thinking through the consequences.

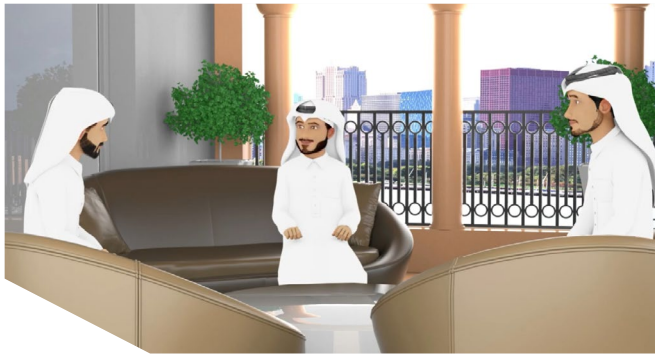
# Cyber 365..

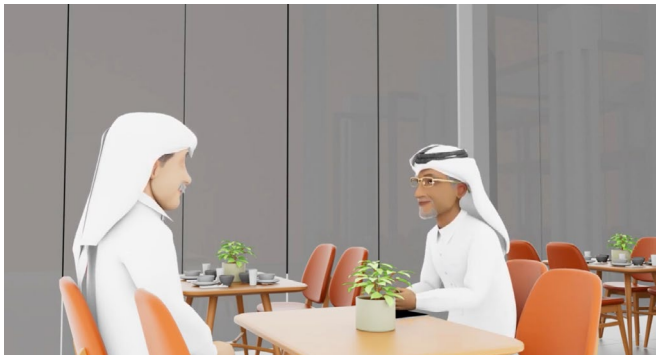
# Pressing Topics and Modern Concepts

As part of the National Initiative for Digital Safety, visual educational content on digital safety topics is delivered to the target groups under the title Cyber 365. This awareness programme includes a variety of video segments, with each group receiving content tailored to its work, lifestyle, and specific cybersecurity awareness needs. This helps increase engagement with the visual material, strengthens its long-term impact, and supports individuals in improving their digital behaviour—helping the initiative achieve its goals for each group.

The Cyber 365 video segments cover a range of topics, including sensitive data security, donation fraud, protecting children from harmful digital content, phishing, online shopping safety, and the security of social media platforms, among others.







# "The Cybersecurity Woman".. Raising Awareness of Safe Online Shopping Principles

Printed interactive games are of strong interest to people across different age groups, and for this reason, they have been included as one of the awareness and training tools of the National Initiative for Digital Safety.

One of the most prominent games is the Cybersecurity Woman game, designed to raise awareness among women and family group about the basics of safe online shopping, the most common and secure digital payment methods, and how to respond to online financial fraud-helping protect data and money from breaches and theft.

The game aims to teach women the fundamentals of cybersecurity in an engaging and interactive way, increase their awareness of how to protect their personal information online, and show them how to apply this knowledge. It also supports decision-making skills in different online security situations and challenges they may face while shopping online. Participants encounter scenarios such as tempting offers and various digital payment methods, using printed cards that simulate online shopping and real-life situations women often experience.

# Cyber City...

# The Secure Digital City


Electronic games are among the most effective tools for raising awareness, as they deliver educational content in a flexible and engaging format that helps individuals gain the greatest possible benefit. For this reason, The National Cyber Security Agency has developed a variety of electronic games under the National Initiative for Digital Safety, aimed at educating target groups about digital safety.

One of these games is Cyber City, designed for expatriate workers. The game takes place on a construction site in a digital city, where the environment includes icons such as hand tools, electrical equipment, buildings under construction, technology devices, and a control and monitoring room. Players move through the site to complete construction tasks and, during the game, face different cybersecurity puzzles that must be solved to earn points and continue. The game provides a clear and simple experience based on direct question-and-answer interactions, suited to the educational and cultural background of expatriate workers.

# The Coordination Meeting...

## Supporting Collaboration Between Partners

As part of The National Cyber Security Agency's commitment to realising the sustainable positive impact of the National Initiative for Digital Safety, the Agency convened a coordination meeting with the initiative's partners on Monday, 26 May 2025. The meeting focused on reviewing the outcomes achieved to date, clarifying communication channels, and coordinating efforts between the Agency and its partners.

It also addressed the action plan and implementation schedule for the mobile stand, including preparations for its upcoming activities.

# News and photos from awareness-raising workshops

# Qatar Society for Rehabilitation of Special Needs

On Thursday, 22 May 2025, the National Cyber Security Agency conducted an awareness-raising workshop at the Qatar Society for Rehabilitation of Special Needs, titled 'Online Identity Theft'. The workshop addressed concepts related to electronic identity theft, the most common types of identity theft, motives for such attacks, their negative effects on internet users, ways to prevent identity theft, and steps to take if identity theft occurs.

# Qatar National Bank (QNB)

On Monday, 26 May 2025, The National Cyber Security Agency conducted an awareness-raising workshop for employees of Qatar National Bank (QNB) under the title "Digital Safety in Financial and Banking Institutions." The workshop covered concepts related to digital safety in financial and banking services, the most common types of cybersecurity challenges in the sector, digital and knowledge-based vulnerabilities that can be exploited to carry out attacks, and the role of employees in preventing such incidents and ensuring digital safety within their institutions.


# Hamad Bin Khalifa University

جامعة حمد بن خليفة
HAMAD BIN KHALIFA UNIVERSITY
عضو في مؤسسة قطر
Member of Qatar Foundation

On Thursday, 29 May 2025, The National Cyber Security Agency conducted an awareness-raising workshop at Hamad Bin Khalifa University, focusing on "Mobile Applications and Privacy Protection." The workshop informed students about key concepts related to mobile applications, the most common associated risks, the types of user data secretly collected through these applications and the reasons behind such practices. It also highlighted the main indicators of malicious software on mobile devices and provided guidance on how to protect personal privacy when using these applications.



Thursday, 2 Dhul-Hijjah 1446 AH, 29 May 2025 CE

# The Second Week of the Awareness-Raising Workshops

## Activities conducted in the second week

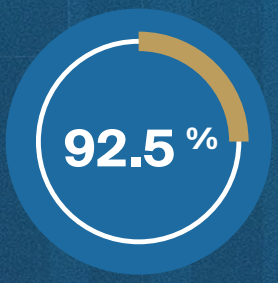
- Presentation of awareness content
- Presentation of Visual Awareness Content
- Distribution of Training Booklets


# The Second Week of Awareness-Raising Workshops....

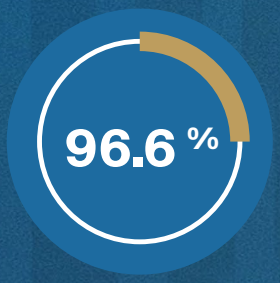
# Outcomes and Impressions

As part of the awareness-raising workshops conducted under the National Initiative for Digital Safety, electronic surveys were distributed to participants in the workshops held during the second week. The aim was to assess the level of benefit gained from the awareness content, and to gather participants' impressions of the trainers' performance and of the initiative overall.

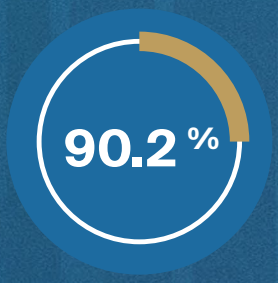
## Engagement with the Awareness-Raising Content




of participants considered the awareness content clear and comprehensible.




of participants demonstrated awareness of cyber risks and the appropriate preventive measures.




of participants rated the initiative as outstanding.

## Perceptions of the teachers' performance

**96.6 %** of participants considered the teachers effective in delivering the awareness content.


QNB