وزارة التنمية الاجتماعية والأسرة
Ministry of Social Development and Family
State of Qatar • دولة قطر

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

International Campaign to Challenge Violence Against Women and Girls

Women's Digital Security

Target Group
Women



الحملة الدولية السنوية
لمناهضة العنف ضد المرأة
حملة 16 يوم

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

International Campaign to Challenge Violence Against Women and Girls

Women's Digital Security

Target Group

Women

Teacher's Booklet

Table of Contents	Page number
Focus area 1: Principles of Digital Security	6
Concept of Digital Security	7
The Importance of Digital Privacy	8
Safe Use of Devices	9
Privacy Settings	10
Data Protection	11
Interactive Question 1	12
Focus Area 2: Key Digital Threats to Women and Girls	13
Key Types of Digital Threats to Girls	14
Measures to Protect Girls from Digital Threats	16
Key Types of Digital Threats to Women	17

Table of Contents	Page number
Measures to Protect Women from Digital Threats	18
Key Types of Digital Threats to Senior Citizens	19
Measures to Protect Senior Citizens from Digital Threats	20
Key Types of Digital Threats to Maids	21
Measures to Protect Maids from Digital Threats	22
Interactive Question 2	23
Interactive Question 3	24
Focus Area 3: Reporting Threats	25
Digital Evidence Documentation	26
Reporting Threats	27
Interactive Question 4	28

Table of Contents	Page number
Focus Area 4: Women's Digital Empowerment	29
Raising awareness of women's rights in cyberspace	30
Initiatives to support women in cybersecurity	31
The role of the National Cyber Security Academy in women's digital empowerment	33
Interactive Question 5	37
Answers to Interactive Questions	38
References	40

Focus area 1

Principles of Digital Security



Concept of Digital Security

Digital security is the ability to use modern technologies and the internet safely and responsibly to protect women's privacy and secure their data against threats and abuse.
It aims to empower women to engage confidently in cyberspace free from fear of exploitation or tracking.

It includes securing personal devices and data.

It enhances users' confidence in using online platforms.

By raising awareness and promoting preventive measures, it helps minimise risks before they arise.



The Importance of Digital Privacy

Digital privacy is the protection of personal data against unauthorised access, whether by individuals or third parties.For women, digital privacy is essential to psychological safety and social wellbeing

Measures to ensure digital privacy

Avoid sharing photos or other sensitive information on public platforms.

Review privacy settings regularly for each app.



Do not accept friend requests from people you do not know.

Think before you post—digital content can be difficult to remove.

Safe Use of Devices



Smart devices are now integral to women's daily lives, so keeping them secure is a priority.

Enable a fingerprint lock or set a strong passcode for your device.

Keep your operating system and apps up to date.

Turn on the device-location feature—'Find My' or 'Find my device'—in case of loss or theft.

Do not install apps from unknown sources.

Privacy Settings



Social media provides a space for expression, but it is also an open environment that can expose women to risk if their online presence is not managed with care.

Turn on two-factor authentication (2FA)—also known as two-step verification—to protect your accounts.

Set who can see your posts—and who can interact with them.

Revoke access for untrusted apps connected to your account.

Avoid sharing your real-time location while travelling or on the move.

Review your social media privacy settings and choose who can see your posts.

Only accept friend requests from people you know.

Limit how often you share everyday personal details online.

Data Protection



Family photos and chats are among the most sensitive types of personal data.

- Use secure messaging apps with end-to-end encryption (E2EE).
- Delete old messages—especially those containing personal data.
- Avoid sending sensitive photos or documents by email or over public messaging channels.
- Keep encrypted backup copies of important data.
- Do not store sensitive photos on devices connected to the internet.
- Use an app with built-in encryption to store your private photos securely.
- Regularly delete duplicate or unnecessary photos from your devices.

Interactive Question 1



1 What is the best practice for protecting your online accounts?

a. Using the same password for all accounts.

b. Enabling two-factor authentication (2FA) and changing your password regularly.

c. Sharing your password with a trusted friend.

d. Leaving your accounts logged in on public or shared devices.

Focus Area 2

Key Digital Threats to Women and Girls



Key Types of Digital Threats to Girls



Online Harassment
Sending unwanted messages or offensive images.

Online Extortion
Threatening to share images or to fabricate audio or video recordings.

Cyberstalking
Unwanted messages and attempts to compromise accounts.

Key Types of Digital Threats to Girls

Cyberbullying
Abusive or offensive comments.

Digital Identity Theft
Account compromise and theft of personal data.

Online Emotional Manipulation
False promises and the exploitation of trust for harmful purposes.



Measures to Protect Girls from Digital Threats

Personal data should not be shared on social media

Abusive messages should be ignored and the sender blocked.

Privacy settings on social media accounts should be configured.

Friend requests from unknown individuals should not be accepted.

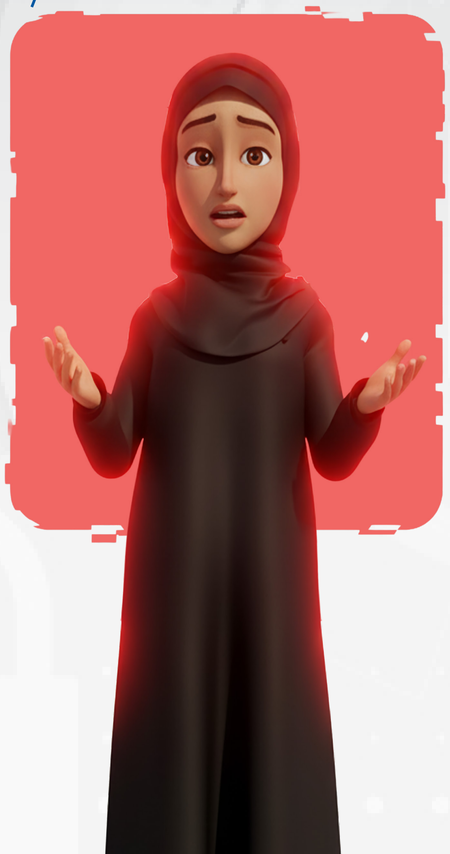


Threats should be documented by retaining screenshots of abusive messages.

Any digital threats should be reported to parents or guardians.

The Ministry of Interior's Economic and Cyber Crimes Combating Department should be notified.

Key Types of Digital Threats to Women



Financial Fraud

Fraudulent e-commerce sites intended to steal financial data.

Personal Data Theft

By installing unsafe applications or sharing personal data.

Malware

Downloading applications from untrusted websites may result in the theft of personal or financial data.

Home Network Compromise

Smart devices, such as internet-connected cameras, can be compromised if they are not protected with strong passwords.

Measures to Protect Women from Digital Threats

Purchases should be made only from official, trusted websites.

Smart home devices should be protected with strong passwords.

Applications should be downloaded only from official, trusted websites.

Personal data should not be shared on social media.

Any digital threat should be reported.

Unknown links should not be opened.

Two-factor authentication should be enabled for social media accounts.



Key Types of Digital Threats to Senior Citizens



Such as spoofed telephone calls or fraudulent messages requesting the transfer of funds or financial data.

Financial Fraud

Fraudulent links on social media platforms such as WhatsApp or Facebook.

Fraudulent links

Renders some women easy targets for social engineering attacks.

Limited technical knowledge

Measures to Protect Senior Citizens from Digital Threats

Links from unknown sources should not be opened.



Personal or financial data should not be shared on social media platforms.

A family member should be consulted before undertaking any new technical action.

Any digital threat should be reported.

Key Types of Digital Threats to Maids



- **Cyber Extortion**

By exploiting her photographs or telephone calls.

- **Financial Fraud**

Fraudulent payment links or spoofed requests for assistance from ‘friends’.

- **Unintentional sharing of information about one’s family or home.**

This poses a security risk to the family.

Measures to Protect Maids from Digital Threats



Photographs should not be taken inside the home.

Unknown links should not be opened.

Personal data should not be shared on social media.

Permission should be sought before sharing any new information.

Any digital threat should be reported.

Interactive Question 2



2 What is the first action that should be taken upon receiving online threats or extortion attempts?

a. Deleting the account immediately.

b. Sending money to the extortionist.

c. Documenting the messages and retaining them as evidence, then reporting to the relevant authorities.

d. Ignoring the threat and informing no one.

Interactive Question 3



3 Which of the following is considered a safe practice to protect against online financial fraud?

a. Entering card details on any website offering tempting discounts.

b. Purchasing only from trusted websites.

c. Sharing card details with a friend to help with the purchase.

d. Saving the password in the phone's notes.

Focus Area 3

Reporting Threats



Digital Evidence Documentation



Preserving and documenting digital evidence is the most important legal step when responding to online violence.

- Capture screenshots with the date and time visible.
- Do not delete abusive messages or the abusive account—retain them as evidence.
- Save the URLs of the original pages and conversations.
- Contact the relevant authorities in your country.

Reporting Threats

Calling
2347444.

Calling the hotline
66815757.



Email to
cccc@moi.gov.qa

The Ministry of Interior's
'Metrash2' mobile application.

Interactive Question 4



4 In the event of receiving a digital threat within the State of Qatar, which of the following are official channels for reporting?

a. Reporting via the Ministry of Interior's 'Metrash2' mobile application.

b. Posting about the incident on social media.

c. Seeking assistance from a friend online.

d. Ignoring the threat and hoping it will resolve itself.

Focus Area 4

Women's Digital Empowerment



Raising awareness of women's rights in cyberspace



Women are entitled to fundamental digital rights, including privacy, freedom of expression, and protection against exploitation or tracking.

Awareness of these rights enhances women's ability to seek legal protection in the event of infringement.

Digital platforms' user-protection policies should be reviewed.

Any content that infringes privacy or is used without permission should be reported.

Initiatives that promote digital equality and increase women's representation in cyberspace should be supported.

Initiatives to support women in cybersecurity

National Initiatives



المخيـــم الشبابي
السيبراني الصيفي

CyberEco

مَنَاهِج الأَمْن السِّيبْرَانِيّ التَّعْلِيمِيَّة
Cyber Security Curricula Education

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

Initiatives to support women in cybersecurity

Women4Cyber Foundation

A European non-profit organisation that supports women's participation in training and employment, with national offices in several European states.

She@Cyber (Erasmus+ Program)

A European project to train women from non-technical backgrounds in the fundamentals of cybersecurity through free educational platforms.

Cynder Project (OAS)

An initiative in the Americas and the Caribbean to integrate women into cybersecurity policymaking and to enhance the digital skills of women and girls.



The role of the National Cyber Security Academy in women's digital empowerment



The National Cyber Security Academy supports women's digital empowerment through the programs and initiatives it has implemented, as follows:

مَنَاهِج **الأَمْن السِّيبْرَانِيّ** التَّعْلِيمِيَّة
Cyber Security Curricula Education

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

المخيـــم الشبابي
السيبراني الصيفي

CyberEco

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

Designed to reach all segments of society.

Women and families are among the principal target groups.

Providing awareness-raising content that enhances women's digital safety.



Awareness-raising content for women is delivered through:

- Digital Safety Guide
- Family Digital Safety Booklet
- The Cyber Home' digital game
- Awareness-Raising Workshops

مَنَاهِج الأَمْن السِّيبْرَانِيّ التَّعْلِيمِيَّة
Cyber Security Curricula Education

Intended for students at all educational levels.

Provides awareness-raising content for female students.

Enhances girls' ability to use the internet safely.

The project has received several international awards.



The approach and lessons learned are being shared with GCC states for implementation.

The project has been implemented in 433 schools.

A total of 583,000 students have benefited from the awareness-raising content.



CyberEco

- Intended for students at all educational levels.
- Integrates learning with entertainment.
- Provides awareness-raising content for female students.
- The project has been implemented in 207 schools.
- Enhances girls' ability to use the internet safely.
- A total of 10,608 students have benefited from the project.

Initiatives to support women in cybersecurity

It is intended for young male and female students.

Provides awareness-raising and training content for female students.

Enhances awareness of cybersecurity concepts.



Supports and develops cybersecurity talent.

A total of 200 students have benefited from the project.

Includes a variety of awareness-raising and training tools.

Interactive Question 5



5 Which of the following constitutes a fundamental digital right for women in cyberspace?

a. Sharing all her personal data publicly.

b. Waiving her privacy in exchange for using platforms.

c. Privacy and protection against tracking and exploitation.

d. Posting other people's information without their consent.



Answers to Interactive Questions

01

Answer to interactive question 1

b. Enabling two-factor authentication (2FA) and changing your password regularly.

02

Answer to interactive question 2

c. Documenting the messages and retaining them as evidence, then reporting to the relevant authorities.

03

Answer to interactive question 3

b. Purchasing only from trusted websites.

04

Answer to interactive question 4

a. Reporting via the Ministry of Interior's 'Metrash2' mobile application.

05

Answer to interactive question 5

c. Privacy and protection against tracking and exploitation.

References

1. ernest, nonum et al. SOCIAL ENGINEERING: UNDERSTANDING HUMAN FACTORS IN CYBER SECURITY. International Journal of Convergent and Informatics Science Research. May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326
2. eSafety Commissioner (Australia). Staying safe: Cyberstalking, on site: https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking
3. European Institute for Gender Equality. Cyber violence against women, on site: https://www.eige.europa.eu/gender-based-violence/cyber-violence-against-women
4. European Parliament. (2023). IPOL_STU(2023)743341_EN [PDF]. on site: https://www.europarl.europa.eu/RegData/etudes/STUD/2023743341//IPOL_STU(2023)743341_EN.pdf
5. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware
6. Karnouskos, Stamatis. Artificial Intelligence in Digital Media: The Era of Deepfakes, IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, June 2020, on site: https://ieeexplore.ieee.org/document/9123958

7. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing
8. Kosinski, Matthew. IBM. What is ransomware? Retrieved, on site: https://www.ibm.com/think/topics/ransomware
9. National Cyber Security Centre. Password policy: updating your approach. November 2018, on site: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
10. Startup Defense. Fake software update prompts. on site: https://www.startupdefense.io/cyberattacks/fake-software-update-prompts
11. UN Women. FAQs: Digital abuse, trolling, stalking and other forms of technology-facilitated violence against Iwomen. February 2025, on site: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women
12. United Nations Office on Drugs and Crime. Handling of digital evidence (Module 6), on site: https://www.unodc.org/e4j/ar/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

وزارة التنمية الاجتماعية والأسرة
Ministry of Social Development and Family
State of Qatar • دولة قطر

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الحملة الدولية السنوية لمناهضة العنف ضد المرأة

حملة 16 يوم

