الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety
Protecting Devices and Data

Target Group
Women

Teacher's Booklet

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Protecting Devices and Data

Target Segment

Women

Teacher's Booklet

Table of Contents	Page number
Introduction	8
The National Initiative for Digital Safety	10
Chapter One: Fundamentals of Digital Safety	13
Concept of Digital Safety	14
Securing Personal Data	15
Safe Use of Smart Devices	16
Password Management	17
Two-Factor Authentication	18
Public Wi-Fi Networks	19
Indicators of Compromise	20
Actions to take in case of a compromise	21
Email Security	22
Social Media Security	23

Table of Contents	Page number
Safe Online Shopping	24
Applications and Digital Services	25
First Interactive Question	26
Second Interactive Question	27
Third Interactive Question	29
Fourth Interactive Question	29
Chapter Two: Digital Threats and Preventive Measures	30
Phishing	31
Malicious Links and Fraudulent Websites	32
Ransomware	33
Malware	34
Social Engineering	35

Table of Contents	Page number
Deepfakes	36
Digital Identity Theft	37
Scam Text Messages	38
Risks of Free Apps	39
Malicious “System Update” Apps	40
Cloud Storage	41
Misleading Advertising	42
Privacy Settings	43
Security Updates	44
Fifth Interactive Question	45
Interactive Question Six	46
Answers to the Interactive Questions	47

Introduction

Digital safety is fundamental to ensuring information security and protecting individuals and communities against ever-increasing cybersecurity threats.

This booklet is intended to raise women's awareness of digital safety principles and best practices to help them avoid risks in cyberspace.



It aims to enhance women's understanding of the most common technological threats they may encounter in daily life, such as phishing, malware, ransomware, social engineering, deepfakes, and digital identity theft.

The booklet also provides practical guidelines and preventive steps for securing personal devices, protecting online accounts, and responding appropriately to any signs of compromise or suspicious activity.

These efforts are part of the National Initiative for Digital Safety, organised by The National Cyber Security Agency, to establish a secure digital environment for all members of society.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative



Initiative Overview

A range of awareness-raising activities in digital safety and cybersecurity for the local community, across all age groups, social segments, and professional sectors. These activities promote awareness of digital safety, encourage the safe use of the internet and technological applications, explain potential risks, and support the development of a society that is secure in cyberspace and technologically capable.

Targeted Groups

The Initiative targets various segments of society with a first-year focus 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

Awareness-Raising Tools

The Initiative employs a diverse, integrated set of awareness-raising tools as follows:

- Digital Safety Guide
- Awareness-Raising Booklets
- Cybersecurity games



- Awareness-Raising Videos
- Innovative Educational Games
- Awareness-Raising Workshops

Chapter One

Digital Safety Essentials



Concept of Digital Safety

Digital safety is the foundation of safe and responsible use of modern technologies. Its goal is to protect women's personal data from risks that may arise during interaction with the digital world.



- It preserves the confidentiality, integrity, and availability of information
- It includes both technical practices such as encryption and updates. and behavioural practices such as avoiding untrusted links
- It empowers women to navigate the digital space confidently and responsibly
- It helps reduce risks before they occur, not after damage is done



Securing Personal Data

Personal data is among the most sensitive assets in the digital world. It includes anything that reveals identity or personal or family details.

Personal data includes names, photos, phone numbers, and banking information

It is recommended to minimize sharing of personal data online and restrict visibility on public platforms



App privacy settings should be reviewed periodically



Encrypted backups of important documents should be stored in safe locations

Safe Use of Smart Devices

Smart devices have become an essential part of a woman's daily life, but they can also be a primary entry point for cyber risks if not properly secured.



Security Practices

- Set a strong password or use biometric authentication to prevent unauthorized access
- Avoid downloading apps from untrusted sources.
- The operating system and applications should be kept up to date to patch security vulnerabilities.
- Enable the "Find My Device" feature to help recover the device if lost

Password Management

Passwords are a foundational element of account protection and are often targeted first by attackers. Managing them wisely is a critical part of digital safety.

Passwords should be long, complex, and unique for each account

Avoid using personal details such as date of birth or name



Use reputable password management tools to store passwords securely

Changing passwords regularly— especially after any suspicious activity

Two-Factor Authentication

Adding a second layer of protection is one of the most effective modern practices for securing accounts. Two-step verification provides strong resistance against hacking attempts—even if the password is exposed.

Requires entering a verification code sent to the phone or email after the password



Recommended for email, banking accounts, and social media platforms

Protects against random login attempts or phishing attacks

Using authentication apps is preferred over SMS for stronger security

Public Wi-Fi Networks

Although public Wi-Fi networks in cafés, airports, or hotels are convenient, they are often not secure and can be used to intercept data.

Avoid entering passwords or banking details while connected to public Wi-Fi

Automatic connection to unknown networks should be disabled



Use a VPN to encrypt your connection if necessary

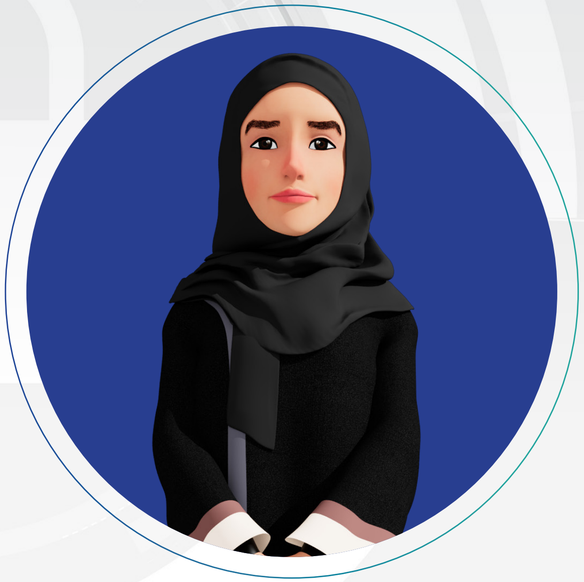
Ensure that any website you use begins with https

Indicators of Compromise

Early detection of signs of compromise is crucial to prevent further damage.

Sudden slowdown in device performance or excessive battery consumption

Unknown programs or pop-ups appearing without installation



Messages being sent from your email or account without your knowledge

Unexpected changes in settings or login notifications from unfamiliar locations

Actions to take in case of a compromise

When noticing any unusual behaviour on devices or accounts, act quickly and follow important steps to limit the damage.



- Disconnect the device from the internet immediately to prevent data leakage
- Change passwords from another secure device
- Run a full scan using a trusted antivirus software
- Save any digital evidence and report the issue to the technical team or service provider

Email Security

Email is one of the most widely used tools in a woman's digital life, but it is also one of the most commonly exploited channels in cyberattacks.

- Verify the sender's address before opening any attachment or link
- Avoid downloading unexpected attachments, even from known contacts, without prior confirmation
- Do not use personal email for professional or public interactions
- Delete suspicious emails immediately and do not reply

Social Media Security



Social media platforms are an essential part of women's digital presence but also require careful and responsible use.

- Enable two-factor authentication for every account
- Review apps connected to your account and remove unnecessary ones
- Control who can see your posts or send you messages
- Avoid sharing location or daily personal details publicly

Safe Online Shopping

E-commerce is an increasingly common part of daily life, which requires careful handling of financial and personal information.



- Buy only from trusted, well-known online stores
- Ensure the website uses (https) before making any payment
- Use virtual or low-limit cards whenever possible
- Avoid entering payment information on public devices or networks

Applications and Digital Services

Smartphones contain dozens of applications that connect to the internet and access user data, making it essential to assess their reliability.

- Read the privacy policy and permission details before installing any app
- Monitor battery and data usage to identify suspicious applications
- Disable unnecessary permissions such as camera or location access
- Regularly delete unused or untrusted applications



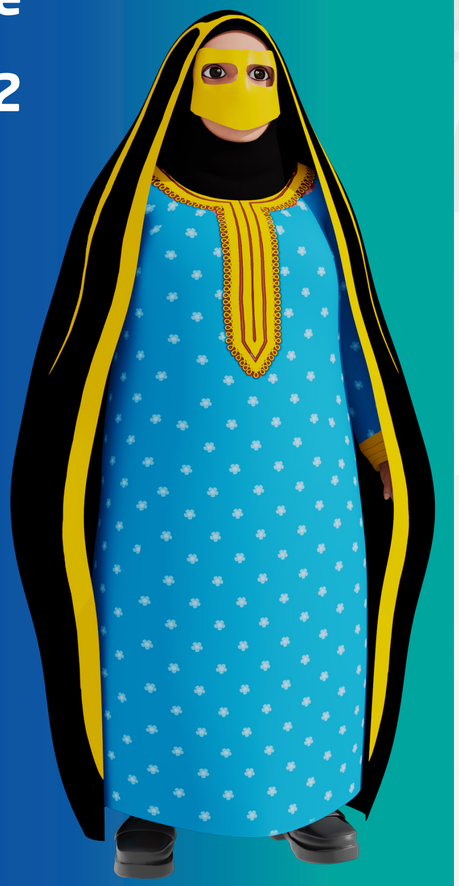
Interactive Question 1



1 **What is the most appropriate action when noticing unusual activity on your account?**

- **A.** | Ignore the notification
- **B.** | Change the password immediately from a secure device
- **C.** | Delete the application without further action
- **D.** | Share the issue with friends

Interactive Question 2



2 **Which of the following practices is most secure when using public Wi-Fi networks?**

- **A.** | Conducting banking transactions immediately after connecting
- **B.** | Using a VPN and avoiding entering sensitive information
- **C.** | Sharing passwords with others
- **D.** | Keeping automatic network connection enabled

Interactive Question 3



2 **Which of the following practices is most secure when using public Wi-Fi networks?**

- **A.** | Conducting banking transactions immediately after connecting
- **B.** | Using a VPN and avoiding entering sensitive information
- **C.** | Sharing passwords with others
- **D.** | Keeping automatic network connection enabled

Interactive Question 4



4 **Which of the following is the safest practice when online shopping?**

- **A.** Enter banking information on any site offering discounts
- **B.** Use public Wi-Fi while completing a purchase
- **C.** Share payment details with the store via email to speed up processing
- **D.** Use low-limit payment cards and confirm the site's security before paying

Chapter Two

Digital Threats and Preventive Measures



Phishing

Phishing is one of the most widespread forms of deception. It involves sending messages or links that appear legitimate, but are designed to steal information.



Fraudulent messages are typically delivered via email, text messages, or fraudulent websites.

These messages request the input of important data such as passwords or card numbers.

They employ a persuasive approach, using urgent or threatening language.

Suspicious messages should be ignored, and their source verified prior to any interaction.

Malicious Links and Fraudulent Websites



Deceptive websites that simulate the interfaces of retailers or official institutions are widespread, designed to mislead users.

They may feature domain names resembling the authentic sites, often with subtle variations.

They are employed to harvest login credentials or payment details.

The reliability of the website can be verified via its address (URL) or its security certificate (https)

It is preferable to access websites directly through a search engine, rather than from received links

Ransomware

Ransomware is malicious software that encrypts files and demands a ransom payment to decrypt them.

Ransomware is commonly delivered via email attachments or suspicious links.

Ransomware prevents users from accessing their files once a device is infected.



Even after paying the ransom, there is no guarantee that the data will be recovered.

Effective prevention includes maintaining regular backups and avoiding attachments from unknown sources

Malware

Malware comprises a range of programs installed on devices to cause damage or steal data.

Malware can be concealed within seemingly legitimate applications or files

Malware can slow the system, steal passwords or monitor user activity

Malware prevention includes installing antivirus software and keeping it up to date

Avoid downloading software from untrusted websites



Social Engineering

Social engineering targets human behaviour rather than technical vulnerabilities, using deception and psychological manipulation.



Attackers may impersonate support staff or claim to represent an official organisation.

attackers harvest information from social media profiles to build rapport with users and then deceive their targets

Social engineering leverages emotional triggers—such as urgency or pressure—to elicit sensitive information

Verify the recipient's identity before sharing any data

Malware

Deepfake technology is an AI-based technique that generates highly realistic synthetic images or videos that closely mimic genuine content.

- Deepfakes may be used to impersonate individuals or to disseminate misleading content
- Deepfakes are difficult for the average user to detect without specialised analysis tools
- Verify the source before reposting any content
- Use deepfake-detection tools and digital media analysis software



Digital Identity Theft

Identity theft occurs when someone obtains personal data and uses it to impersonate the victim.

Identity theft can involve stealing account credentials, payment card numbers, email accounts and more

Personal data may be used to commit financial fraud or social-engineering scams

Minimising the sharing of personal data reduces the risk of identity theft

Regularly monitor your financial accounts to detect unauthorised activity early

Scam Text Messages



Smishing is a form of phishing that uses SMS text messages to deceive recipients.

They include links that claim you've won a prize or ask you to update your bank details

Clicking them could lead to data theft or the installation of malware

Do not open links from unknown senders

Contact the sender directly using an official channel to confirm the message is genuine

Risks of Free Apps

Some applications offer attractive services but collect users' personal data without clear, informed consent.



- It requests permissions that exceed its actual requirements
- It may track location data or record activity in the background
- Always read the privacy policy before installing any application
- Regularly uninstall unnecessary or suspicious applications

Fake 'system update' software

Attackers send fake notifications to trick users into thinking their device needs an immediate update.



Clicking the link can result in malware being downloaded onto the device

Only official updates should be installed via the device settings

Do not download any executable file from an email or an unknown website

Regular system updates help close security vulnerabilities

Cloud Storage

Cloud storage provides practical, on-demand access to files, but it can pose risks if misused.



Uploading unencrypted sensitive files puts them at risk of theft

Sharing public links may inadvertently grant others access

Use reputable cloud services and enable two-factor authentication (2FA)

Regularly delete old files from cloud storage accounts

Misleading Advertising

Some sponsored online advertisements are used to deliver malicious links.

They may claim to offer discounts or instant rewards

Clicking them may lead to pages that attempt to install malware on your device



Avoid clicking on untrusted or clickbait adverts

Using ad-blocking browser extensions can improve security

Privacy Settings

Ignoring privacy settings allows strangers to access personal information.

- Social media privacy settings should be reviewed and visibility controls specifying who can see posts should be configured.
- Only friend requests from known and trusted accounts should be accepted.
- Sharing everyday personal details online should be minimised
- Configure location settings to prevent automatic tracking



Security Updates

Regular software updates are the last line of defence against new threats.

Delaying updates leaves the device vulnerable to new malware

Enable automatic updates for all applications and operating systems

Updates include patches for vulnerabilities that may be exploited in cyberattacks



Restart the device after updating to ensure protection is fully applied

Interactive Question 5



5 **Which of the following statements best describes ‘social engineering’?**

A. | Using file-encryption software

B. | Deceiving users into voluntarily disclosing their information

C. | Breaching the system through a technical vulnerability.

Interactive Question 6



6 **What is the best measure to prevent ransomware infection?**

- **A.** Regular backups should be maintained and suspicious attachments avoided
- **B.** Opening attachments in any incoming email
- **C.** Neglecting to back up files
- **D.** Installing any free application available online



Answers to the Interactive Questions

01

Answer to the first interactive question

b. Change the password immediately from a secure device

02

Answer to the second interactive question

b. Using a VPN and avoiding entering sensitive information

03

Answer to the third interactive question

c. Verify the sender's identity before opening the attachment, or delete it if unsure

04

Answer to the fourth interactive question.

d. Use low-limit payment cards and confirm the site's security before paying

05

Answer to the fifth interactive question

b. Deceiving users into voluntarily disclosing their information

06

Answer to interactive question six

a. Regular backups should be maintained and suspicious attachments avoided



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466798 - 51045944

www.ncsa.gov.qa/ academy@ncsa.gov.qa