الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Group

Senior Citizens

Teacher's Book

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Group

Senior Citizens

Teacher's Book

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

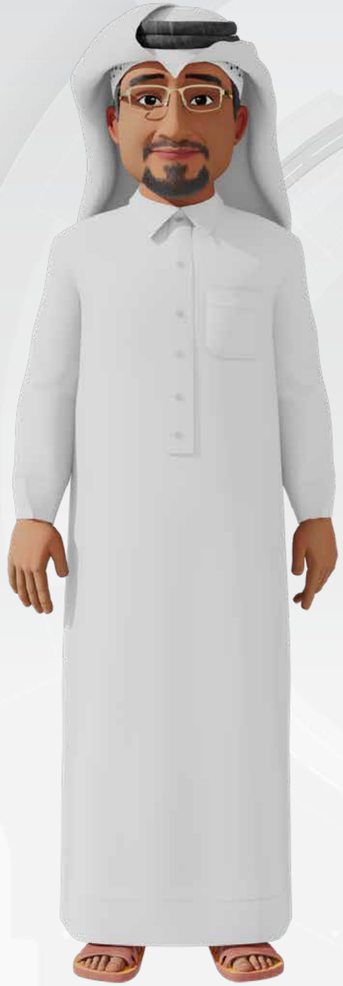
Contact the National Cyber Excellence Department

00974 404 663 79
00974 404 663 62
www.ncsa.gov.qa/
academy@ncsa.gov.qa

Table of Contents	Page number
Introduction	7
Scope of the Initiative	8
Targeted Groups	9
Awareness-raising tools	10
Common Cybersecurity Risks	11
Senior Citizens' Vulnerability to Cybercrimes	12
Real-Life Scenarios of Cybercrimes	13
First Interactive Question	17
Risks of Social Media Platforms	18
Second Interactive Question	20
Social engineering	21
Information and Data Sought in Social Engineering Attacks	22
Third Interactive Question	23

Table of Contents	Page number
Phishing	24
Indicators of Phishing Attempts	25
Password Strength	26
Passwords	27
Password Vulnerabilities	28
Security measures for protecting passwords	29
Fourth Interactive Question	30
Fifth Interactive Question	34
Practical Tips	35
How to Respond to Breach Incidents	36
Avoiding Suspicious Links	37
Answers to the Interactive Questions	38

Introduction



Digital safety is an essential element for ensuring information security and protecting individuals and communities from the increasing threats in Cyberspace.

This booklet is designed to familiarise senior citizens with the principles of digital safety and best practices for avoiding cybersecurity threats. It seeks to enhance their awareness of risks such as phishing and malware, and to enable them to protect their data and devices effectively.

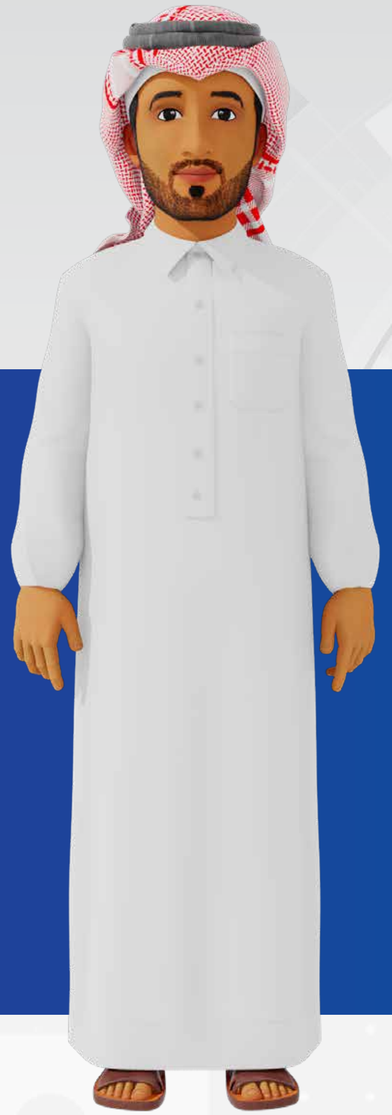
These efforts are part of the National Initiative for Digital Safety, organised by The National Cyber Security Agency, to establish a secure digital environment for all members of society.

Scope of the Initiative

A set of awareness activities in digital safety and cybersecurity, targeting the local community across all age groups, social backgrounds, and professional sectors.

The initiative aims to raise awareness of digital safety and the secure use of the Internet and various technological tools while clarifying potential risks, with the goal of building a society that is secure in cyberspace and capable in the use of technology.

Targeted Groups



The initiative addresses all societal groups. During its first year, primary focus will be directed towards 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 set of varied and integrated awareness tools, which include the following:

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

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

Common Cybersecurity Risks

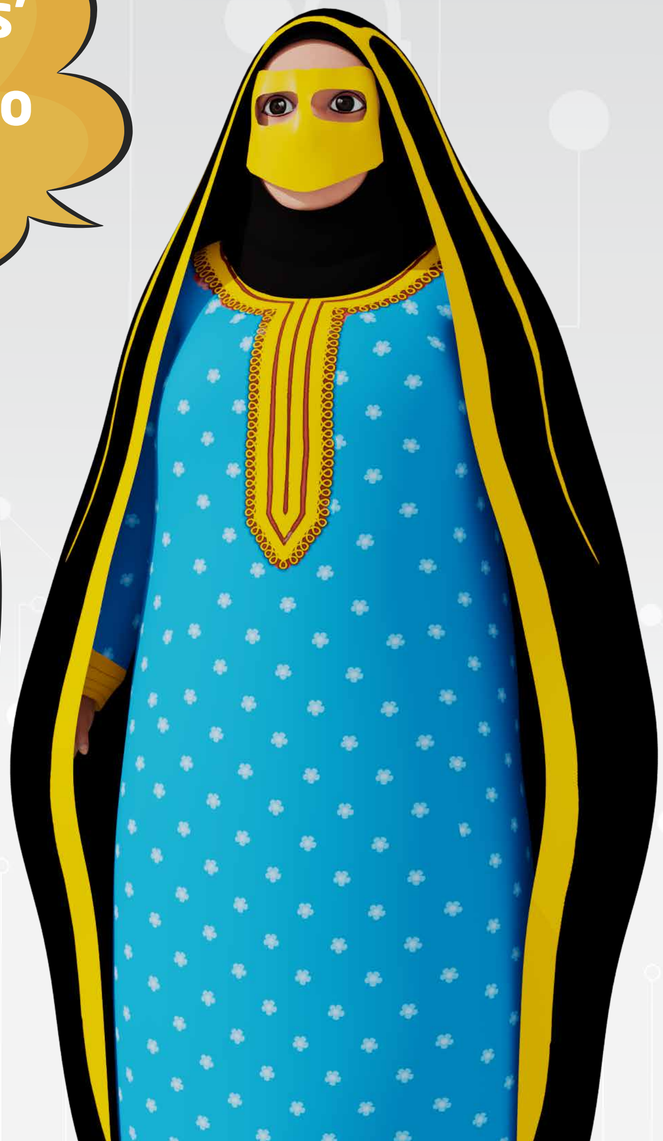
Senior Citizens' Vulnerability to Cybercrimes

Senior citizens are generally targeted by cyber attackers for several reasons:

Limited technical knowledge:
Senior citizens often lack sufficient awareness of cybersecurity threats, such as phishing and malware

Reliance on technology:
As senior citizens make greater use of online banking and internet-based communication, they become more vulnerable to cyberattacks

Trust-based vulnerability:
Senior citizens are typically more trusting and may engage with fraudulent communications, such as phone calls or emails, without verifying their source



Real-Life Scenarios of Cybercrimes

Banking fraud involving fraudulent messages claiming to be from banks

The victim receives a text message or email purporting to be from a well-known bank, requesting an update of their personal information. Once the information is entered, the attacker gains unauthorised access to the victim's bank account.

Real-Life Scenarios of Cybercrimes

Unauthorised access to social media accounts

The victim receives a direct message via social media platforms, containing a suspicious link purporting to be from the platform's administration. After clicking the link, the attacker gains control of the account.

Real-Life Scenarios of Cybercrimes

Phishing attack involving a fraudulent delivery company

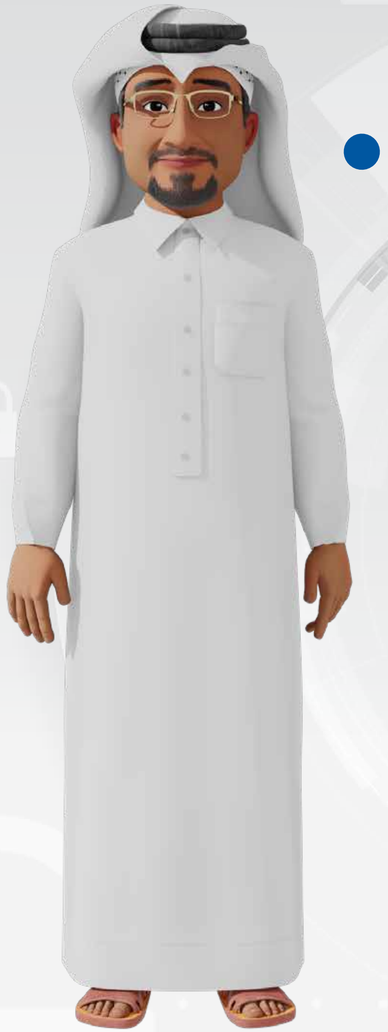
The victim receives a message stating that a shipment is awaiting payment of fees or requires an update of data. If the victim enters their card details, the information is stolen by the attacker.

Real-Life Scenarios of Cybercrimes

Unauthorised access to the home Wi-Fi network

Hackers take advantage of weak security settings in a home Wi-Fi network, allowing them to intercept communications, access personal devices, and steal sensitive data.

First Interactive Question



1 **What is the correct action to take when you receive a call from someone claiming to be from the bank and asking for your account information?**

A. Provide the information immediately to avoid any issues.

B. End the call immediately without asking any questions.

C. Verify the caller's identity by contacting the bank directly.

D. Send your account number via text message to ensure the request is genuine.

Risks of Social Media Platforms

Sharing personal information on social media may expose users to the risk of data theft and the unauthorised use of their information.

Personal information shared on social media platforms may be used to carry out phishing attacks.

Protection

Configuring privacy settings to reduce the risk of unauthorised access to your personal information

Avoid unverified links and suspicious messages

Using strong, unique passwords and enabling two-factor authentication to protect accounts

Second Interactive Question

2 What is the best course of action when you receive a friend request from a stranger on social media?

A. Accept the request.

B. Ignore the request.

C. Delete the request.

D. Send a message to the person who sent the request.

Social engineering

Social engineering is not a cyberattack by definition but a set of techniques and tools employed by attackers to deceive their victims.

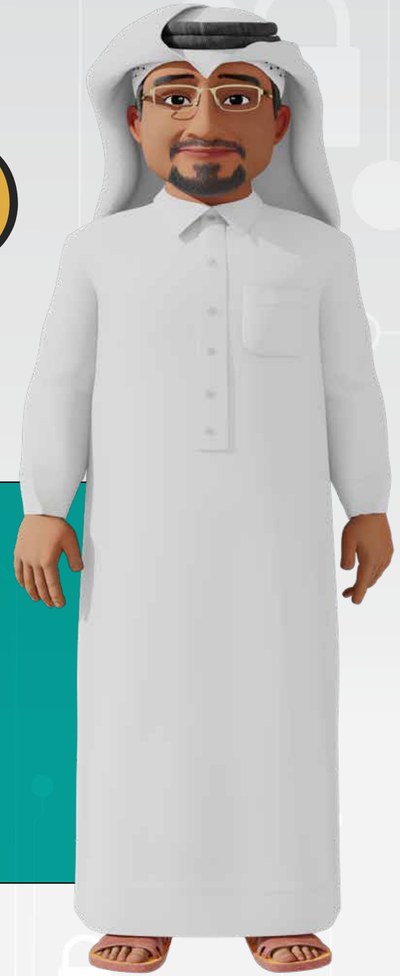
In social engineering, attackers exploit human emotions such as fear, desire, need, and compassion, as well as other emotional triggers.

Attackers exploit human emotions to deceive victims into disclosing sensitive information, which is then used for fraudulent purposes.

Beware!

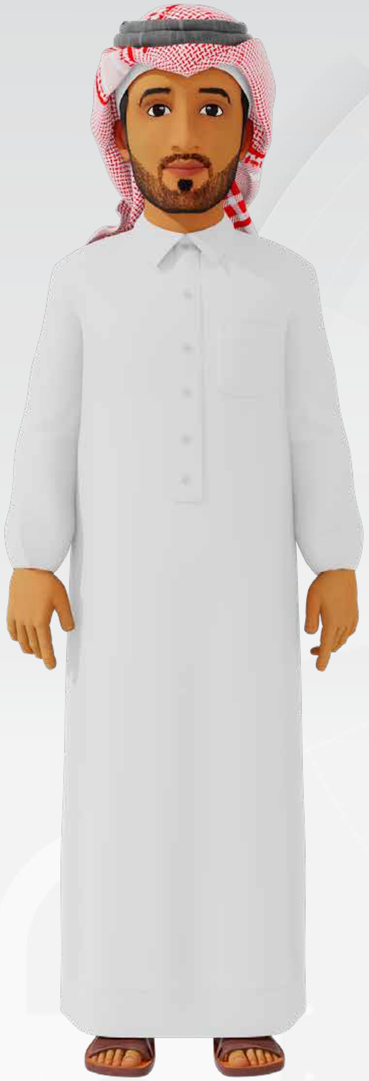
Beware of fraudulent calls and messages, and never share your OTP with anyone.

Information and Data Sought in Social Engineering Attacks



Attackers use social engineering attacks to obtain the following information:

- Social security numbers
- Phone numbers
- Bank account information
- Personal information
- Sensitive work-related information



Third Interactive Question

3 What should you do if you receive a suspicious WhatsApp message requesting sensitive information?

A. Respond immediately and send the requested information.

B. Inquire about the requested information.

C. Verify the sender's identity before taking any action.

Phishing

Phishing is a type of fraud in which attackers impersonate a trusted individual or entity through email or other forms of communication.

Attackers use emails to deliver malicious links designed to collect sensitive information, such as bank account numbers or personal data related to family or work.

Beware!

Make sure to monitor your bank accounts regularly to ensure there is no suspicious activity.

Indicators of Phishing Attempts

- A writing style that is unfamiliar to the recipient
- Grammatical and spelling errors
- An unusual request for personal and sensitive information
- Inconsistencies in email addresses and links
- Suspicious attachments
- A request to download software or click on links
- Messages claiming you have won a prize

Key Facts and Information

A key vulnerability that attackers exploit to compromise passwords is users' tendency to use simple and easily guessed passwords, such as those made up only of numbers or letters, or to neglect updating them regularly.

Password Strength

Passwords

Passwords represent the first line of defence against cyberattacks.

Strong passwords consist of lowercase and uppercase English letters, numbers, and symbols.

A strong password is made up of more than 12 characters.

The use of easily guessable passwords may result in the compromise of your data and devices.

Password Vulnerabilities

Common and easily guessable passwords, such as 12345 or password.

Using personal information when creating a password, such as an address or a date of birth.

Using only letters or numbers.

Security measures for protecting passwords

Using password management software.

Enabling two-factor authentication (2FA).

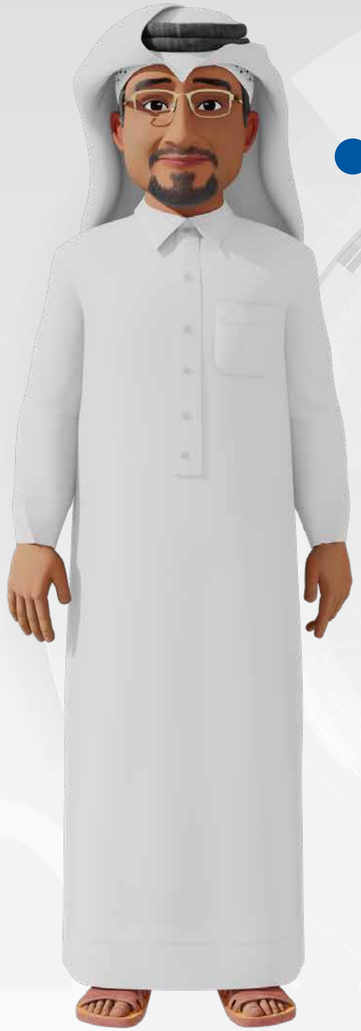
Changing passwords regularly.

Being cautious of phishing messages.

Writing your password on paper or in a file should be avoided; instead, it should be stored in a password management software

Logging out when accessing accounts from shared computers.

Fourth Interactive Question



Which of the following cybersecurity practices are correct and which are incorrect?

1 Using the same password for all accounts to increase security. (correct/ incorrect)

A. correct

B. incorrect

Fourth Interactive Question

2 Using passwords made up of numbers only is sufficient to protect accounts. (correct/ incorrect)

A. correct

B. incorrect

Fourth Interactive Question

3 Password management software can be used to store passwords securely. (correct/ incorrect)

A. correct

B. incorrect

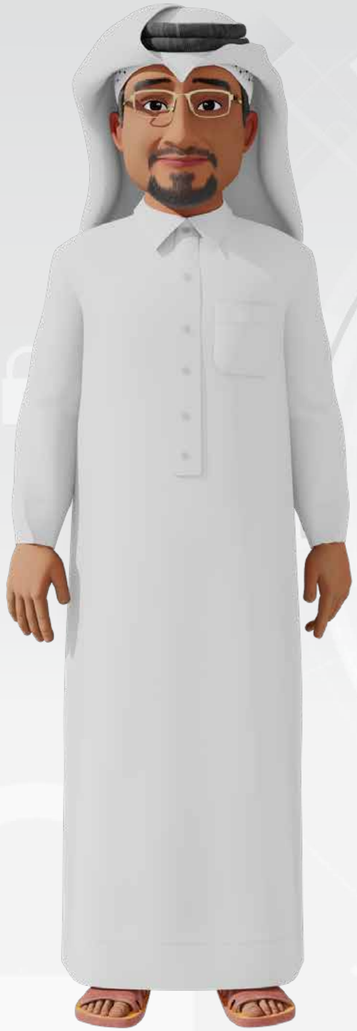
Fourth Interactive Question

4 Choosing a long password that includes a mix of letters, numbers, and symbols is not useful for the user and is difficult to remember. (correct/ incorrect)

A. correct

B. incorrect

Fifth Interactive Question



5 **While browsing the internet, a message appears stating that you have won a grand prize and asks you to enter your details to claim it. What should you do?**

A. I enter my details immediately to claim the prize.

B. I verify the source of the message before doing anything.

C. I share the link with my friends so they can claim the prize too.

D. I ignore the message and exit the website immediately.

Practical Tips

How to Respond to Breach Incidents

There are key steps to follow when responding to a breach:

Change your passwords: Update all passwords immediately, including those for both compromised and uncompromised accounts

Notify the relevant parties: Contact your bank or the affected platform and report the incident promptly

Update your devices and software: Make sure your operating system and security tools are fully up to date to prevent security vulnerabilities

Monitor your accounts: Check your financial accounts regularly to detect and prevent any unauthorised activity

Use antivirus software: Scan your device with reliable software to detect and remove any malware

Avoiding Suspicious Links

Avoid clicking on links contained in unexpected or unfamiliar messages.

Verify the link address before clicking, and make sure it begins with ‘HTTPS’.

Do not click on links from unknown senders or suspicious websites.

Beware of pop-up ads or links that promise large prizes.

Answers to the Interactive Questions

01

Answer to the first interactive question

C) Verify the caller's identity by contacting the bank directly.

02

Answer to the second interactive question

C) Delete the request.

03

Answer to the third interactive question

C) Verify the sender's identity before taking any action.

04

Answer to the fourth interactive question.

1. incorrect.
2. incorrect.
3. correct.
4. incorrect.

05

Answer to the fifth interactive question

D) I ignore the message and exit the website immediately.

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency