الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Introducing Cyber Attacks

Target Audience
Media Professionals

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Introducing Cyber Attacks

Target Segment

Media Professionals

Teacher's Guide

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

To Contact the National Cyber Security Academy

16555
00974 404 66 798
00974 510 45 944
academy@ncsa.gov.qa

Table of Contents	Page number

Introduction

Digital safety is a core element to ensure information security and protect individuals and communities from the ever-increasing cyber threats.

This booklet is designed to educate media professionals on digital safety principles and best practices to help them avoid cyber risks. It aims to raise their awareness of the most significant cyber threats they may encounter in their work, including phishing, ransomware, viruses, social engineering, deepfakes, and digital identity theft.

The booklet also offers best practices and preventive measures to protect devices, secure accounts, and respond promptly to any signs of breach.

These efforts are part of the National Digital Safety Initiative developed by the National Cyber Security Agency to create a secure digital environment for all segments of society.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

About the Initiative

This initiative provides a series of awareness activities in the field of digital safety and cybersecurity targeting the local community that target different age groups, social segments, and professional sectors.

It was launched to raise awareness of digital safety and the responsible use of the internet and diverse technological tools, emphasizing potential risks and aiming to foster a cyber secure, technologically empowered society.

Target Segments

The initiative targets various segments of society, focusing in its first year on the following groups:

Senior Citizens

Women and Family

People with Special Needs

University Students

Expatriate Workers

Civil Society Organizations

Financial and Banking Sector

Awareness-raising Tools

The initiative employs diverse and integrated awareness tools, including:

- Digital Safety Guide
- Awareness Booklets
- Cyber Games
- Awareness Videos
- Innovative Educational Games
- Awareness Workshops

First Chapter

Digital Safety Fundamentals

Digital Safety Concept

Digital safety is the set of procedures and practices that enable media professionals to protect their personal and professional data when using devices and the Internet.

Basic Elements of Digital Safety

Providing device protection from hacking and malicious software

Maintaining confidentiality of journalistic information sources

Ensuring communication security during press coverage and investigations

Preventing unauthorized access to data

Building trust between journalists and the public through a secure digital environment

Common Digital Threats

Media professionals face diverse digital attacks designed to steal, distort, or mislead.

Prominent threats

- Email and SMS phishing

- Malware and Ransomware

- Social engineering based on deception

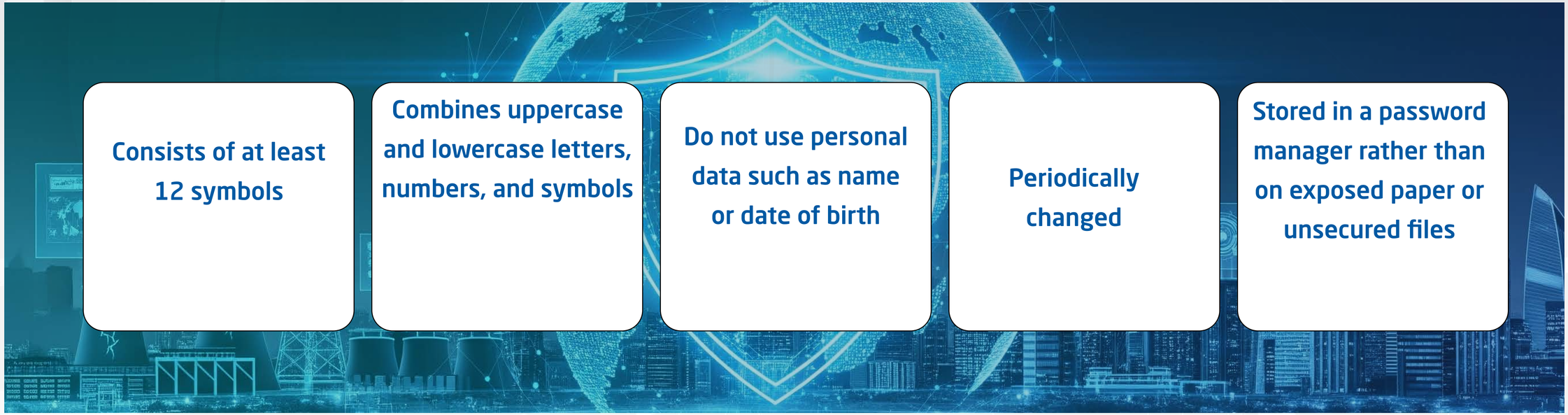
- Eavesdropping on communications over public networks

- Deepfakes to produce misleading videos or recordings

Passwords

Strong passwords are the first line of defense against any hacking attempt.

Characteristics of Strong Password



Email Security

Email is an essential tool for any media professional, yet the most targeted.

Email Security Practices

Social networking Security

Social media platforms have become a hotbed for hacking.

Tips for protecting accounts

- Limit who can view your posts or comments

- Review Apps linked to account

- Enable login notifications

- Be alert for suspicious messages

- Use different password for each account

Public Network Security

Public Wi-Fi networks pose significant risks for media professionals, particularly during field coverage.

Safe Practices

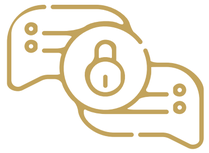
- Use a VPN to encrypt your connection
- Avoid entering passwords or financial data
- Disable auto-networking
- Make sure your website starts with “https”

Protecting Press Sources

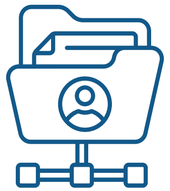
Journalistic sources are very sensitive, that's why they should be treated confidentially.

Methods of Protection

Encryption of shared documents and files



Using secure messaging applications



Separate source data from profiles

Awareness of digital security principles

Signs of Device Breach

- Unusual slow performance of your device
- Pop-up windows or ads
- Sending messages from the mail without your knowledge
- Sudden changes in files or applications
- Login notifications from unfamiliar locations

Initial Procedures When Breach is Suspected

Any suspicious activity should be addressed promptly.

Immediate Action

Disconnect the device from the internet

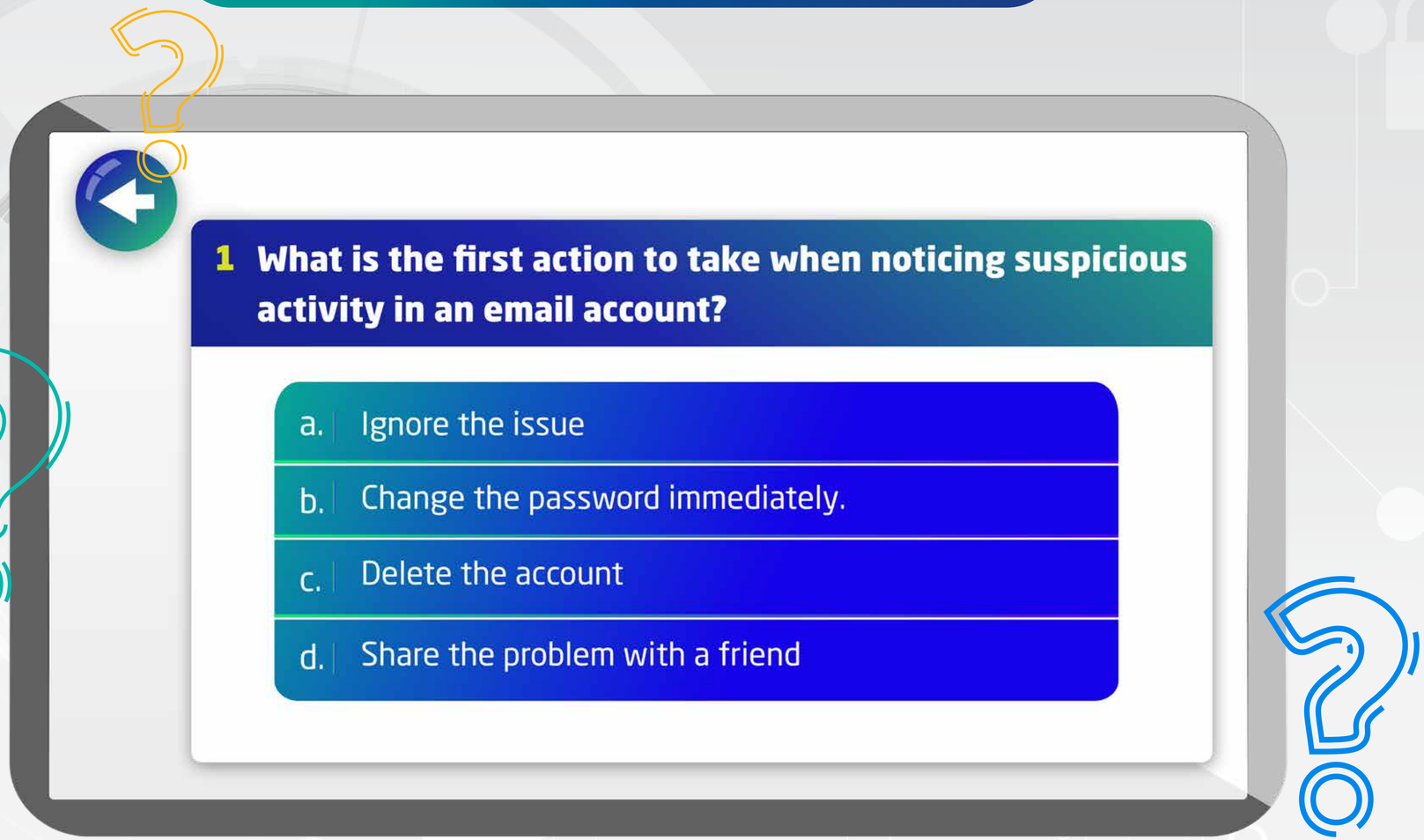
Change basic passwords from another secure device

Notify the technical support team or the management of the media organization

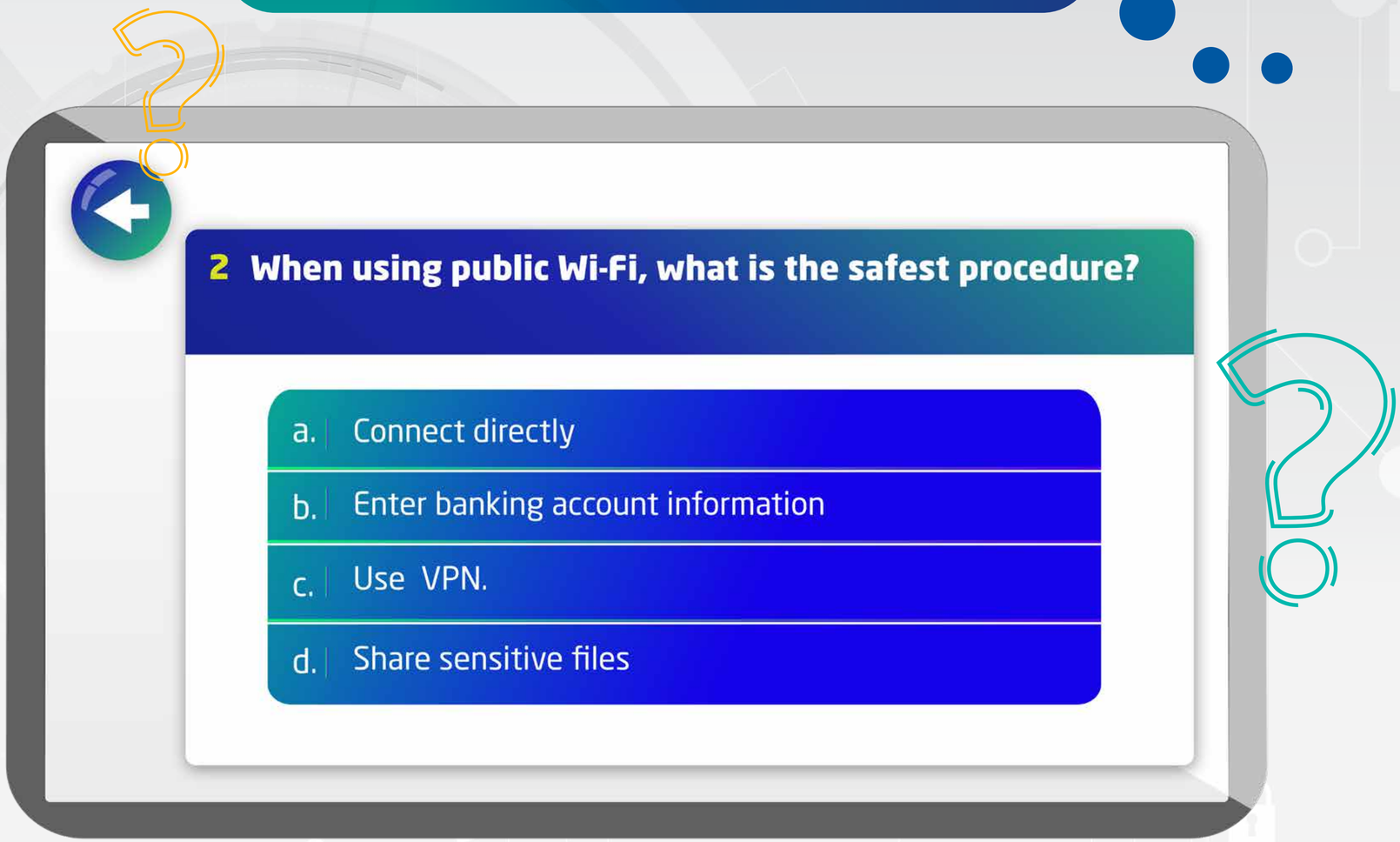
Incident documentation (photos, time, messages)

Conduct a thorough inspection of the device

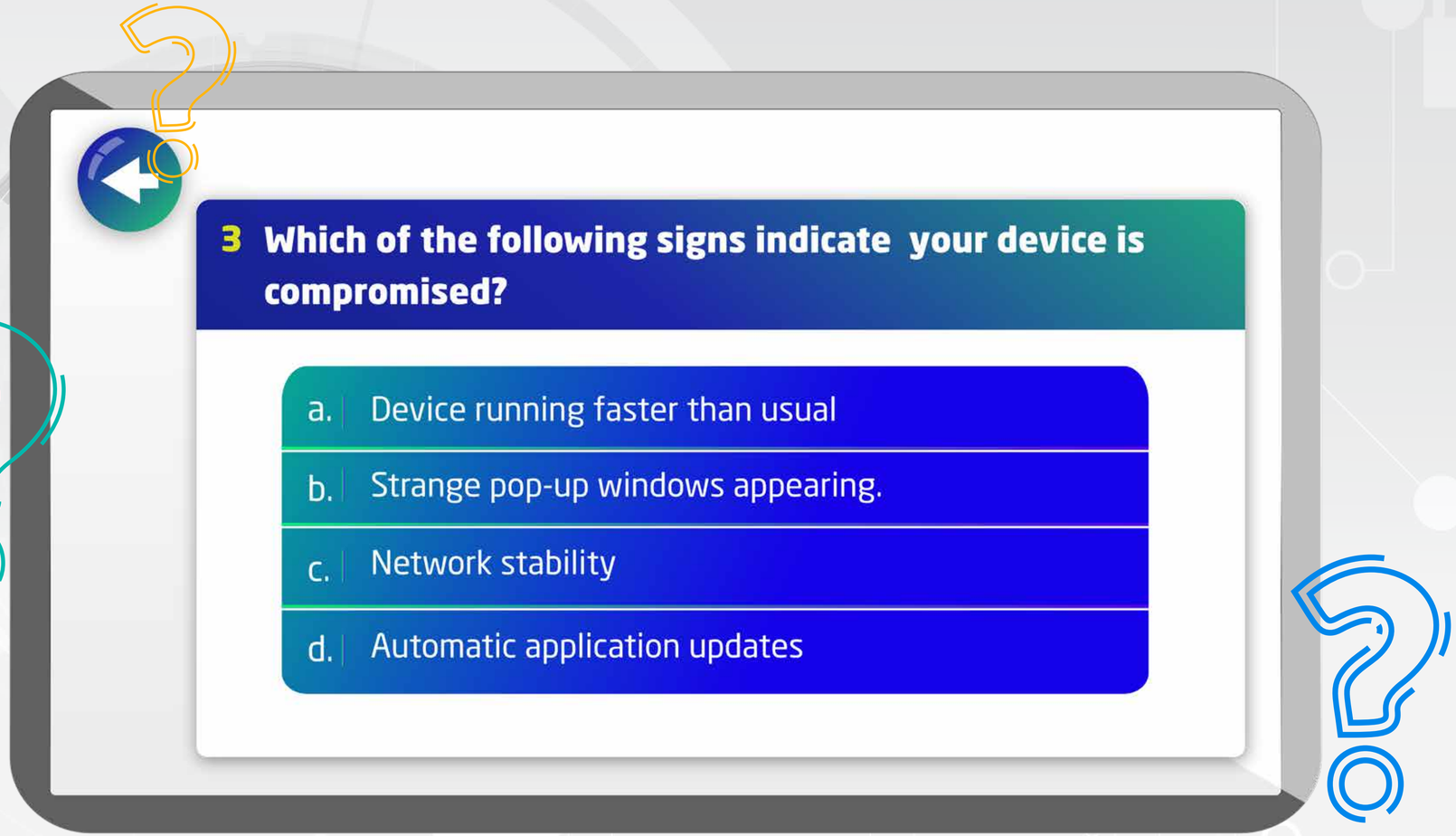
First Interactive Question



Second Interactive Question

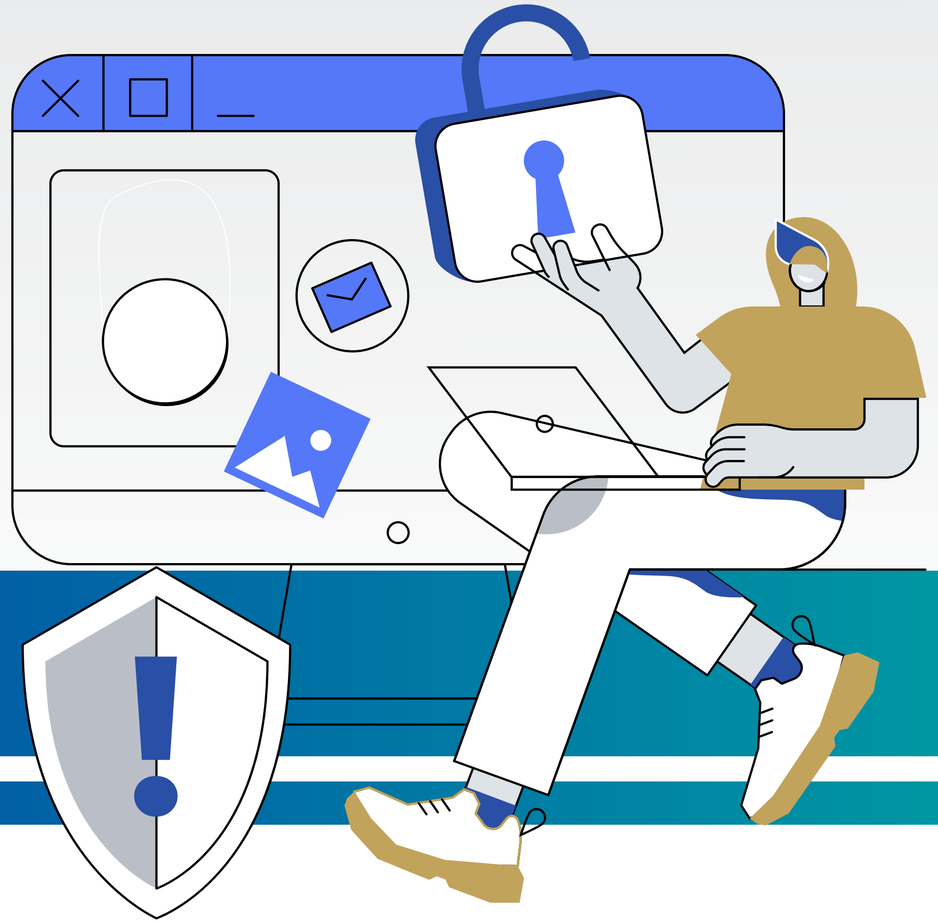


Third Interactive Question



Chapter Two

Cybersecurity Threats and Attacks



Malware

Cyber attackers may deploy malware to damage devices, steal sensitive data, or gain control over content.

Key characteristics

- It is transmitted through suspicious attachments or links
- It may hide itself inside programs or applications that appear to be trusted
- They range from viruses, worms, ransomware, or spyware
- Leads to loss of control over devices or data
- Sometimes used to spy on the work of journalists

Prevention Measures

- Install antiviruses and update them regularly
- Avoid downloading software from untrusted locations
- Don’t click on anonymous links or attachments
- Enable firewall to block attacks
- Conduct a periodic check of the device to ensure that it is free of malware

Viruses

A computer virus is malicious software that infiltrates a device, alters its normal operation, or destroys the data stored on it.

Key characteristics

- Often embedded within files that appear legitimate such as images or documents
- The virus begins to spread when the file is opened or run
- Some viruses cause files to be deleted or the entire system to be disabled
- Transferred from one device to another over the internet or media such as USB

Prevention Measures

- Always use up-to-date antivirus software
- Avoid opening anonymous files
- Scan USB media before running them
- Update operating systems and software to close security vulnerabilities

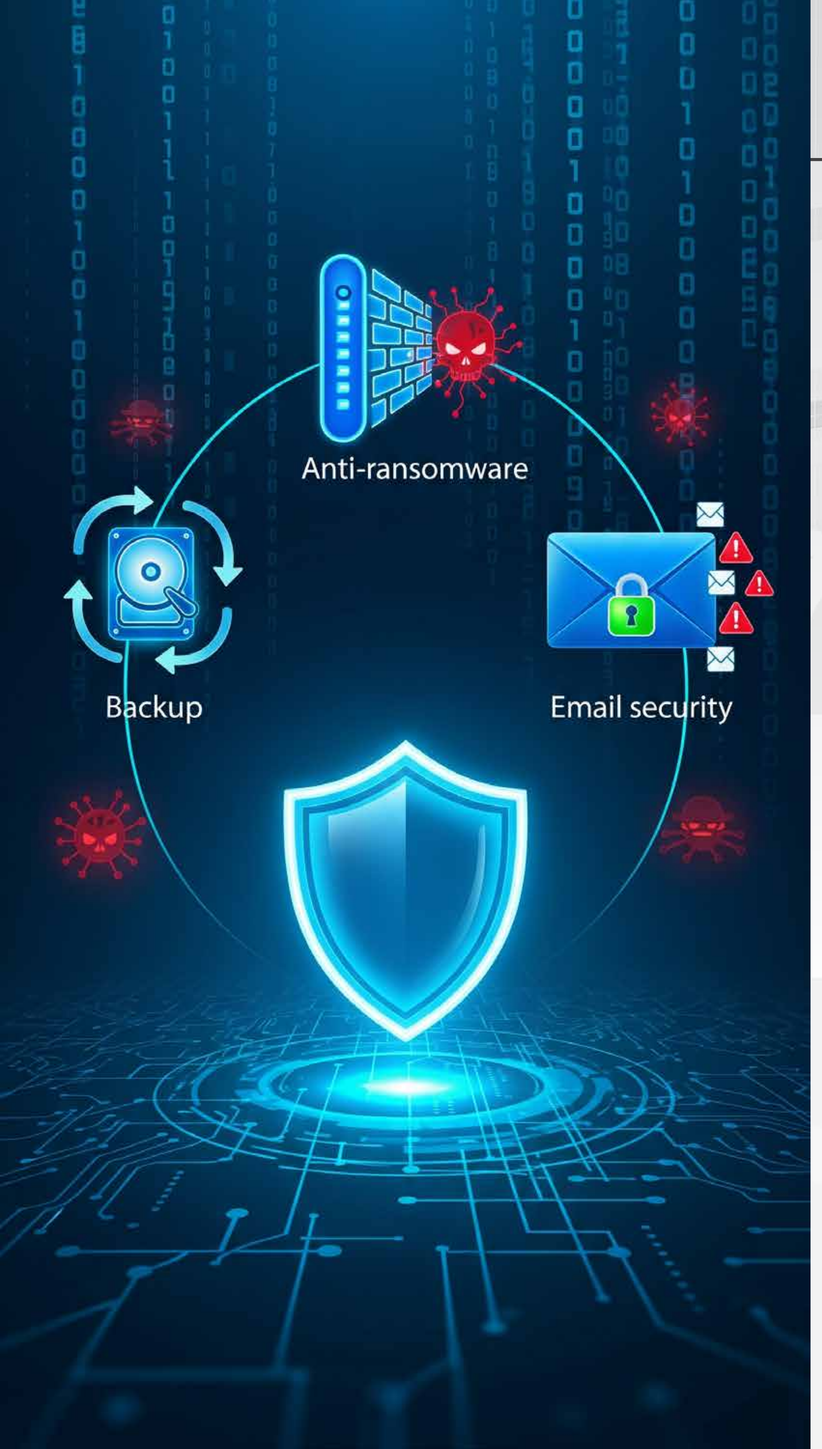
Ransomware

Ransomware is a highly dangerous form of malicious software that encrypts a victim's files and demands a ransom payment in exchange for the decryption key.

Key characteristics

- Typically delivered via email containing malicious attachments
- Once infected, it locks files or the entire system

- Hackers demand ransom payments, usually in cryptocurrency like Bitcoin
- Even after payment, there's no guarantee files will be recovered



Prevention Measures

- Regular backup of critical files
- Use specialized security software designed to prevent ransomware attacks
- Avoid opening attachments from unknown sources
- Keep systems and applications updated to close security bugs

Trojans

A type of malware that infects computers and mobile devices by attaching itself to legitimate programs available online.

Key characteristics

- Creates a backdoor allowing attackers to control the device
- Presented as video editing tools or email management software
- May be used to steal account passwords

Prevention Measures

Download software only from official websites

Monitor device activity and installed programs regularly

Use intrusion detection and antivirus software

Never install unknown or suspicious programs

Phishing

Phishing is a type of cyberattack that uses fraudulent messages or websites made to look legitimate in order to trick people into revealing sensitive information.

Phishing Characteristics

- Often appear as fake emails or text messages
- Request users to enter sensitive data such as passwords or bank card numbers
- Use urgent language like “Your account is suspended, act now!” to prompt immediate action without thinking
- Mimic the design and logos of well-known institutions to appear legitimate
- The primary goal is stealing information for financial exploitation or blackmail

Prevention Measures

Check email addresses and links before clicking on them

Avoid sharing personal data via suspicious messages

Use two-step verification for accounts

Social Engineering

Social engineering is a cyberattack technique that manipulates human emotions, rather than exploiting technical vulnerabilities to deceive users.

Key characteristics

- Pretend to be technical support staff, friends, or officials
- Exploits emotions like fear, sympathy, or embarrassment to prompt responses
- Attackers use persuasion and psychological manipulation to obtain information
- Relies on gathering information from social media to build user trust
- Considered among the most dangerous methods because it requires no technical skills, relying instead on victim behavior

Prevention Measures

- Verify the identity of callers or senders before sharing any information
- Avoid sharing sensitive details with untrusted individuals
- Educate the journalists about the dangers of this technique
- Establish clear verification protocols before responding to any requests

Deepfake

Deepfake refers to the process of using artificial intelligence to produce false but highly realistic content.

Key characteristics

- Creating videos or audio recordings that mimic public figures
- Hard to tell what's real and what's fake

- Can directly damage the reputation of journalists or media outlets
- Often used to spread misleading news that influences public opinion

How to Spot Deepfake Content

Use deepfake detection tools

Look for abnormal movements or sounds

Double-check with multiple trusted sources before sharing any video or audio

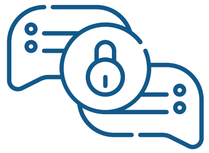
Review the file's metadata

Digital Identity Theft

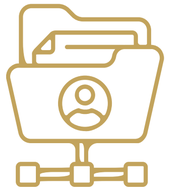
Digital identity theft happens when someone gains unauthorized access to another person's online identity information and uses it illegally for personal or financial gain.

Examples of Stolen Data

Credit card numbers



Passwords



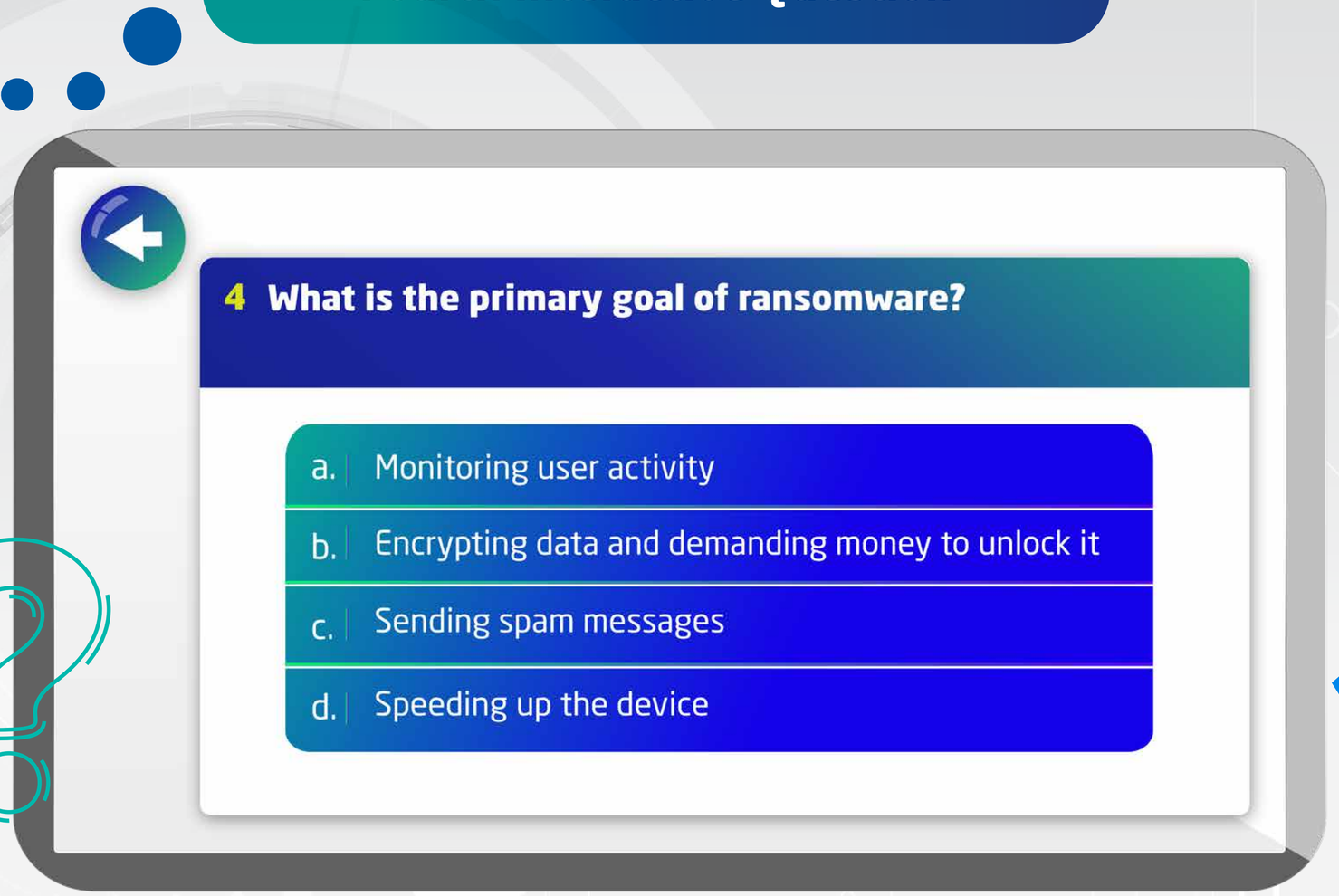
National or social security numbers

Banking information

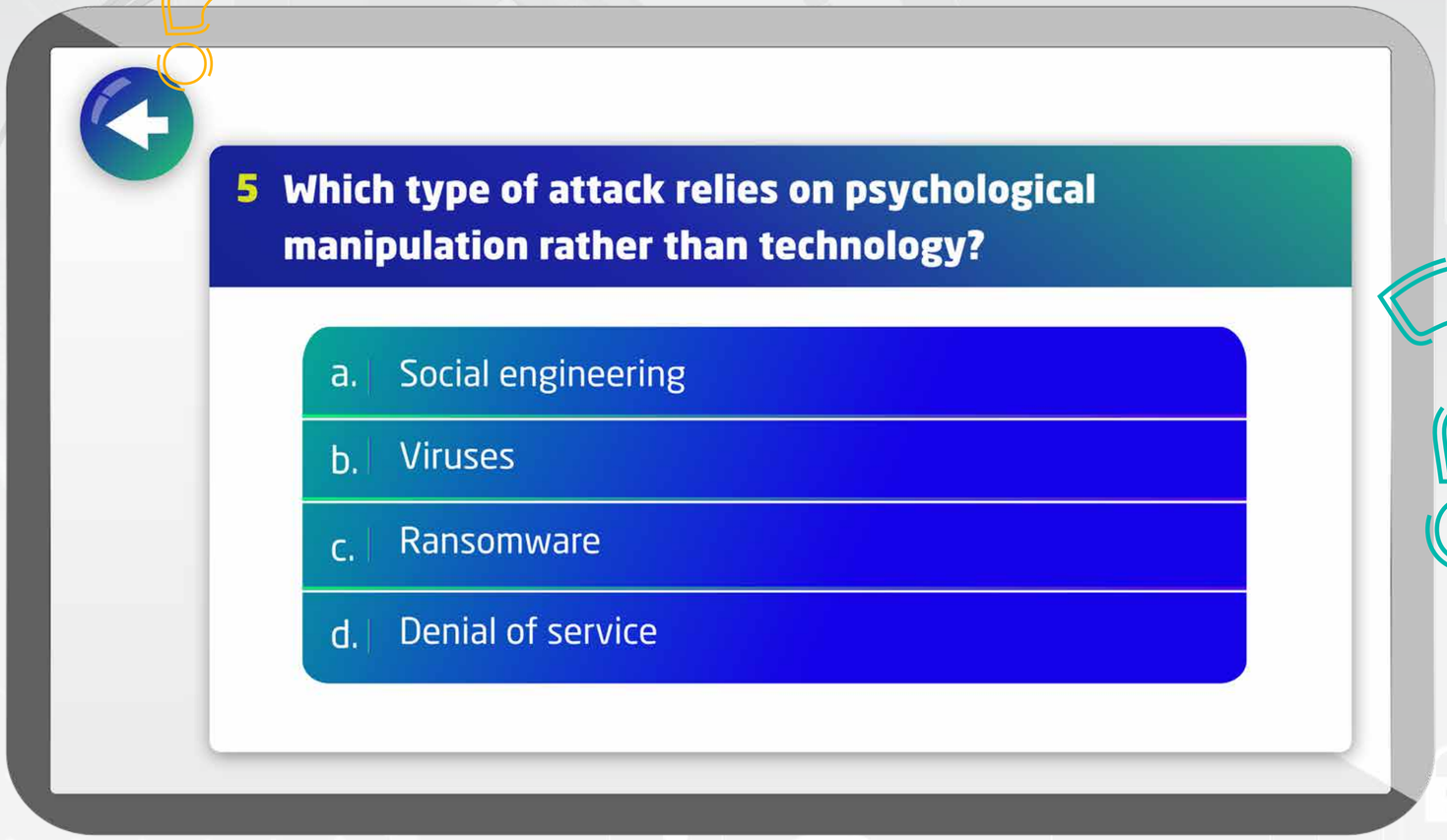
Prevention Measures

- Change passwords periodically
- Avoid sharing sensitive details online
- Check email addresses and links before clicking on them
- Use intrusion detection and antivirus software
- Always use up-to-date antivirus software
- Never share your password with anyone

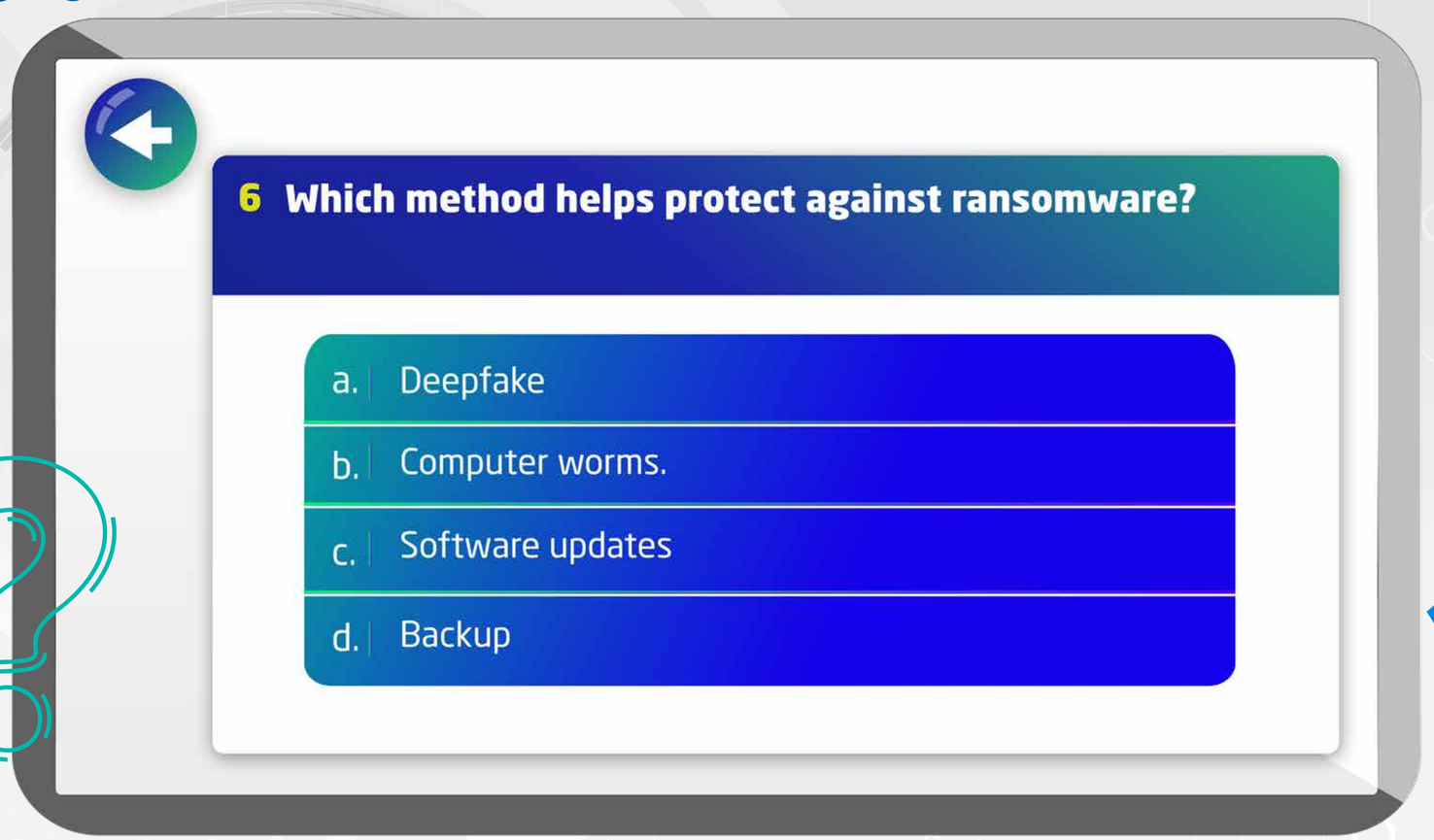
Fourth Interactive Question



Fifth Interactive Question



Sixth Interactive Question



Answers to Interactive Questions

01 **Answer to first interactive question**

b. Change the password immediately

02 **Answer to second interactive question**

c. Use a VPN

03 **Answer to third interactive question**

b. Strange pop-up windows appear

04 **Answer to fourth interactive question**

b. Encrypting data and demanding money to unlock it

05 **Answer to fifth interactive question**

a. Social engineering

06 **Answer to sixth interactive question**

d. Backups

Before closing, please take a moment to fill out your personal information and evaluate the workshop. Scan the below QR code:

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency