الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target group

Penal and Correctional Institutions and the Public Prosecution

Teacher's Guide

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

Target group

Penal and Correctional Institutions and the Public Prosecution

Teacher's Guide

Table of Contents	Page Number

Introduction

In the age of digital transformation, penal and correctional institutions and the public prosecution are no longer merely traditional institutions; they have become complex digital systems exposed to a wide range of cyber risks.

This booklet has been designed to raise awareness among staff in these institutions of the principles of digital safety and the best practices that can help them avoid such risks. It also aims to enhance their awareness of the main cyber threats they may encounter in the course of their work, such as phishing, ransomware, viruses, and digital identity theft.

The booklet also provides best practices and preventive measures for protecting devices, securing accounts, responding promptly to indicators of compromise, and protecting data through encryption.

These efforts form part of the National Initiative for Digital Safety, organised by The National Cyber Security Agency, and aim to create a safe cyberspace for all groups in society.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

Initiative Overview

A range of awareness-raising activities in digital safety and cybersecurity, designed for the local community across different age groups, social groups, and professional sectors.

The initiative promotes awareness of digital safety and the safe use of the internet and technological applications. It also highlights potential risks, helping to create a cyber-secure and technologically capable society.

Target Groups

The initiative reaches diverse segments of society, with a particular focus on the following groups

01 First Year

Senior Citizens

Women and Family

People with special needs

University Students

Expatriate Workers

Civil Society Organisations

The Financial and Banking Sector

02 Second Year

- Media Professionals
- Diplomats
- Athletes
- Penal and Correctional Institutions and the Public Prosecution
- Healthcare Workers
- Women (Digital Violence Against Women)
- General Public

03 Third Year

- Staff at the Ministries of Defence and Interior
- Staff in the energy sector
- Staff in the education sector
- People with special needs
- Teenagers and young adults
- General Public

Awareness-Raising Tools

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

Digital Safety Guide

Printed Awareness-Raising Booklets

Presentation Slides (for teachers)

Animated Awareness-Raising Videos

Live-Action Awareness-Raising Videos

خَـلّك وَاعي
وَعْيك دِرْعك

Cybersecurity Games

Cybersecurity Awareness Portal

Interactive Robot

Awareness-Raising Workshops

Focus Area One

The National Cyber Security Agency and the Protection of the Digital Community

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

Establishment and Objectives

Establishment

"

The National Cyber Security Agency was established under Amiri Decree No. (1) of 2021 as the State's national point of reference for protecting cyberspace. Its mandate is to enhance the State's cybersecurity and ensure the protection of digital assets and critical infrastructure from growing cyber threats.

"

Objectives

Enhancing cybersecurity

Develop advanced policies to ensure the protection of digital systems, and implement comprehensive preventive measures to detect and mitigate cyber threats

Raising Awareness

Organising training programs and awareness-raising campaigns to educate individuals and institutions on the importance of cybersecurity and how to counter cyberattacks

Building National Capacity

Training national professionals in the latest cybersecurity technologies, while supporting research and studies that enhance the State's ability to address cyber challenges

International Cooperation

Establishing partnerships with international organisations and exchanging expertise with leading States in cybersecurity

to combat cybercrime and enhance cyber defences

Vision and Mandate

Strategic Vision

Achieving a safe Cyberspace that supports social and economic development.

Enabling the knowledge economy by enhancing trust in digital services.

Mandate

1. Developing and implementing the National Cyber Security Strategy.
2. Monitoring cyber threats and responding to incidents through specialist teams
3. Establishing technical and regulatory policies and standards to protect digital infrastructure
4. Coordinating national cybersecurity efforts across public and private sector entities.
5. Raising public awareness of cybersecurity through awareness-raising campaigns and training programs.
6. Representing the State internationally in cybersecurity-related forums and agreements.
7. Developing national expertise through training and professional certifications

Protecting Data and Critical Sectors

01 The Agency adopts the latest international standards in data protection to ensure the security of digital systems.

02 The Agency plays a guiding role in ensuring that institutions comply with Law No. (13) of 2016 on Protecting Personal Data Privacy.

03 Developing training programs for public and private institutions to enhance their awareness of data protection and equip their staff to apply the necessary preventive measures.

04 Introducing initiatives to raise users' awareness of their rights to access and protect their data, thereby enhancing transparency and mutual trust between users and institutions.

05 Providing channels for reporting data breaches, while ensuring that complaints are handled promptly and effectively to minimise harm and protect users.

Integrated Approach to Addressing Cybercrime

The National Cyber Security Agency and the Ministry of Interior coordinate their respective roles to protect cyberspace

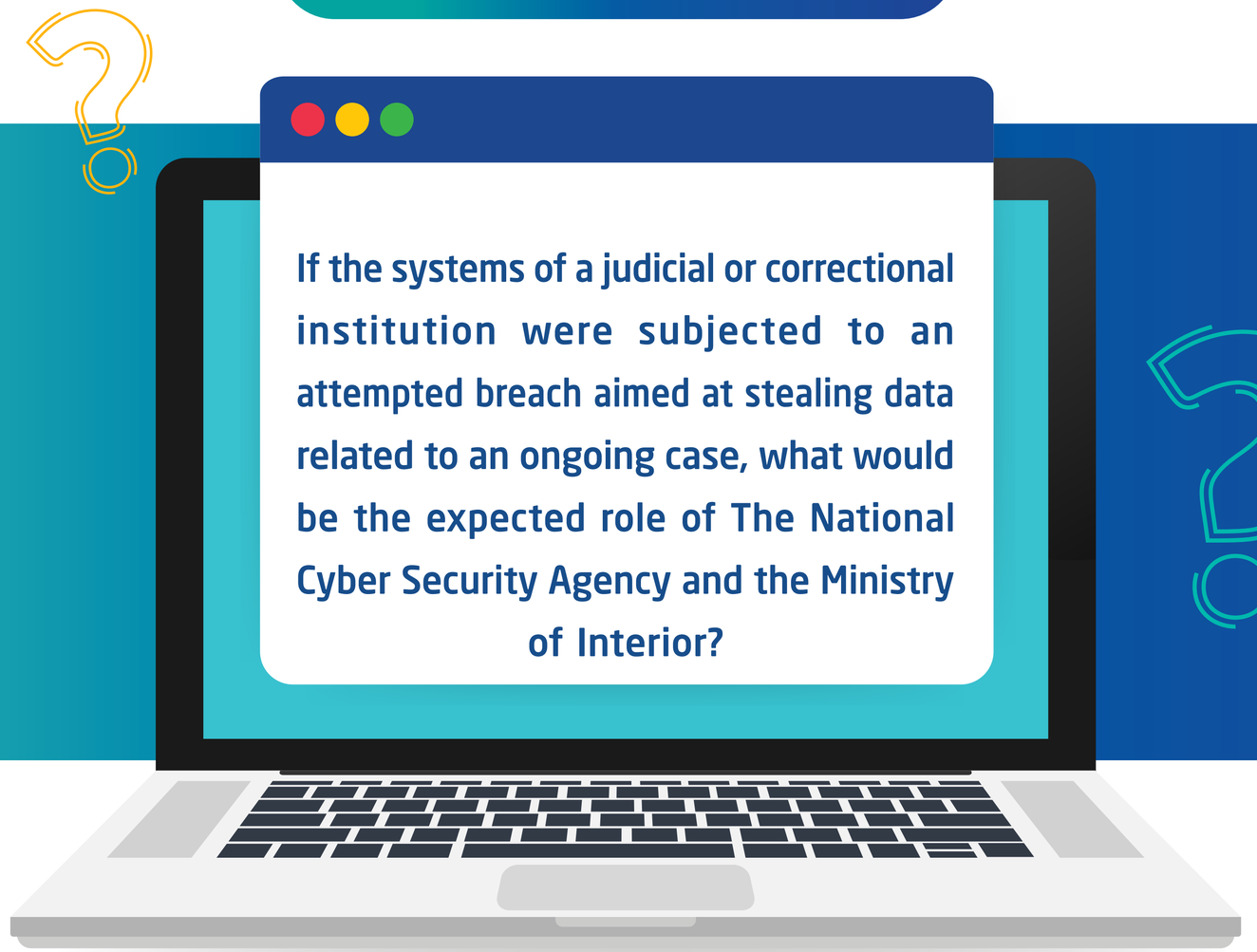
الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

- Introducing national initiatives for digital safety
- Developing policies, standards, and preventive procedures
- Implementing community awareness and education programs
- Providing technical and technological support to various sectors
- Monitoring and tracking digital threats at the national level

وزارة الداخليـــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

- Investigating cybercrime and bringing perpetrators to justice
- Collecting digital evidence in accordance with applicable legal frameworks.
- Protecting society from online criminal activity.
- Coordinating with Interpol and relevant international law enforcement bodies when necessary.
- Enforcing penalties in accordance with relevant laws relating to cybercrime.

Interactive Question



If the systems of a judicial or correctional institution were subjected to an attempted breach aimed at stealing data related to an ongoing case, what would be the expected role of The National Cyber Security Agency and the Ministry of Interior?

Focus Area Two

Common Cyber Threats in the Judicial and Correctional Environment

Targeted Social Engineering

In social engineering, attackers exploit ‘urgency’ and ‘authority’. They may impersonate a senior regulatory body or an internal technical unit, and once the link is clicked or the attachment is downloaded, the institution’s internal network may be compromised.

The objective is often to steal credentials, such as usernames and passwords, in order to gain access to Case Management Systems (CMS) or Inmate Management Systems (IMS).

Facts and Figures

Global reports indicate that the government and judicial sectors were among the sectors most heavily targeted by ransomware in 2023 [1].

1. Federal Bureau of Investigation. (2023). 2023 Internet Crime Report. Internet Crime Complaint Center (IC3). On site: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Phishing Techniques

Malicious Email

Messages impersonating the Ministry of Justice or the police

01

Voice Phishing (Vishing)

A phone call in which the caller claims to be from technical support and asks for the password ‘to resolve an urgent issue’

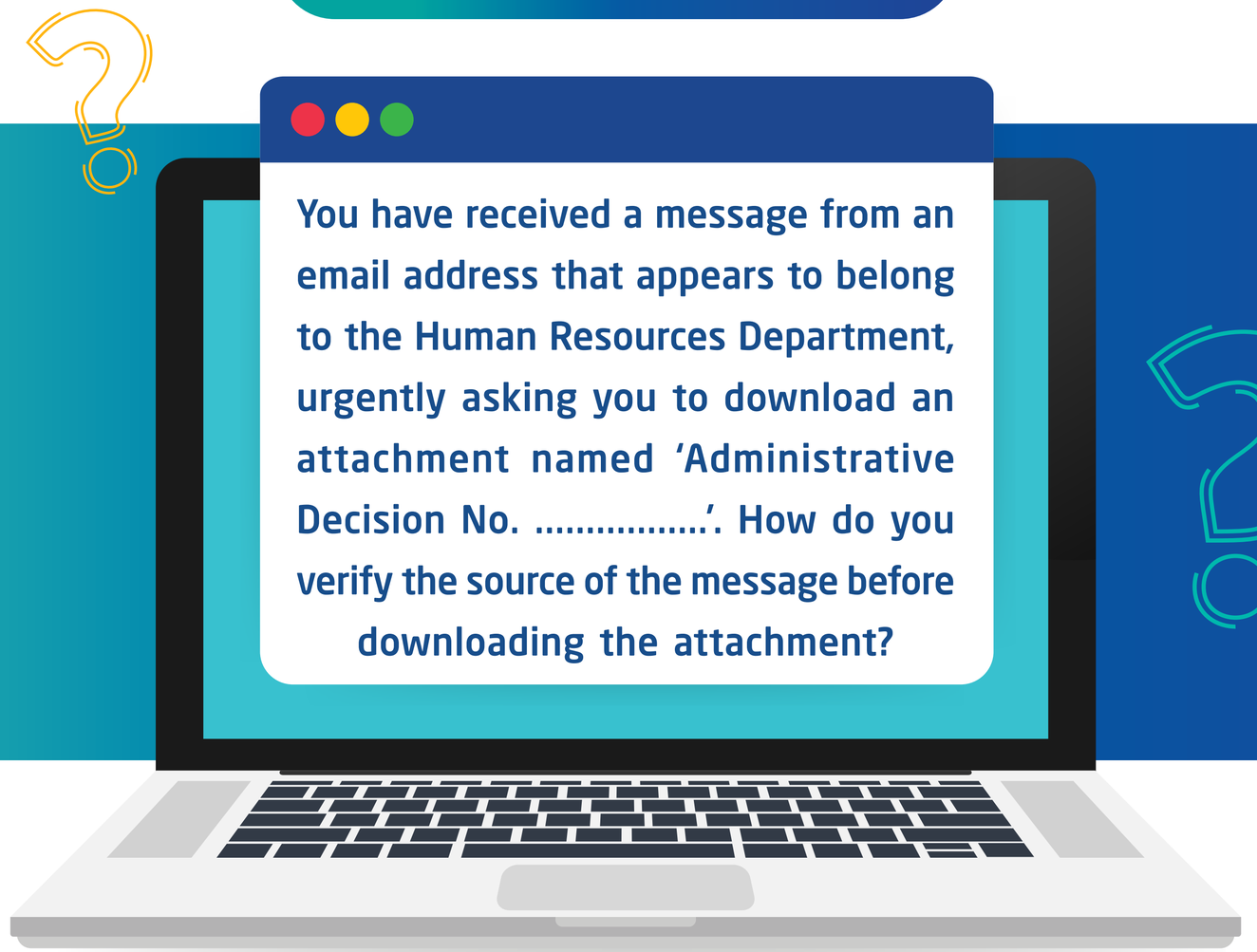
02

Luring Through Social Media

Monitoring employees’ personal accounts to gather information for use in an attack

03

Interactive Question



Ransomware

The malware often gains access through an unpatched vulnerability or a malicious email attachment. It then spreads laterally across the network, encrypting servers and connected backups.

01 For the Public Prosecution

A ransomware attack may bring investigations to a complete halt, lead to the postponement of court hearings, and result in the possible loss or corruption of digital evidence. This may result in charges against some defendants being dismissed due to insufficient evidence caused by its loss or inaccessibility.

02 For Correctional Institutions

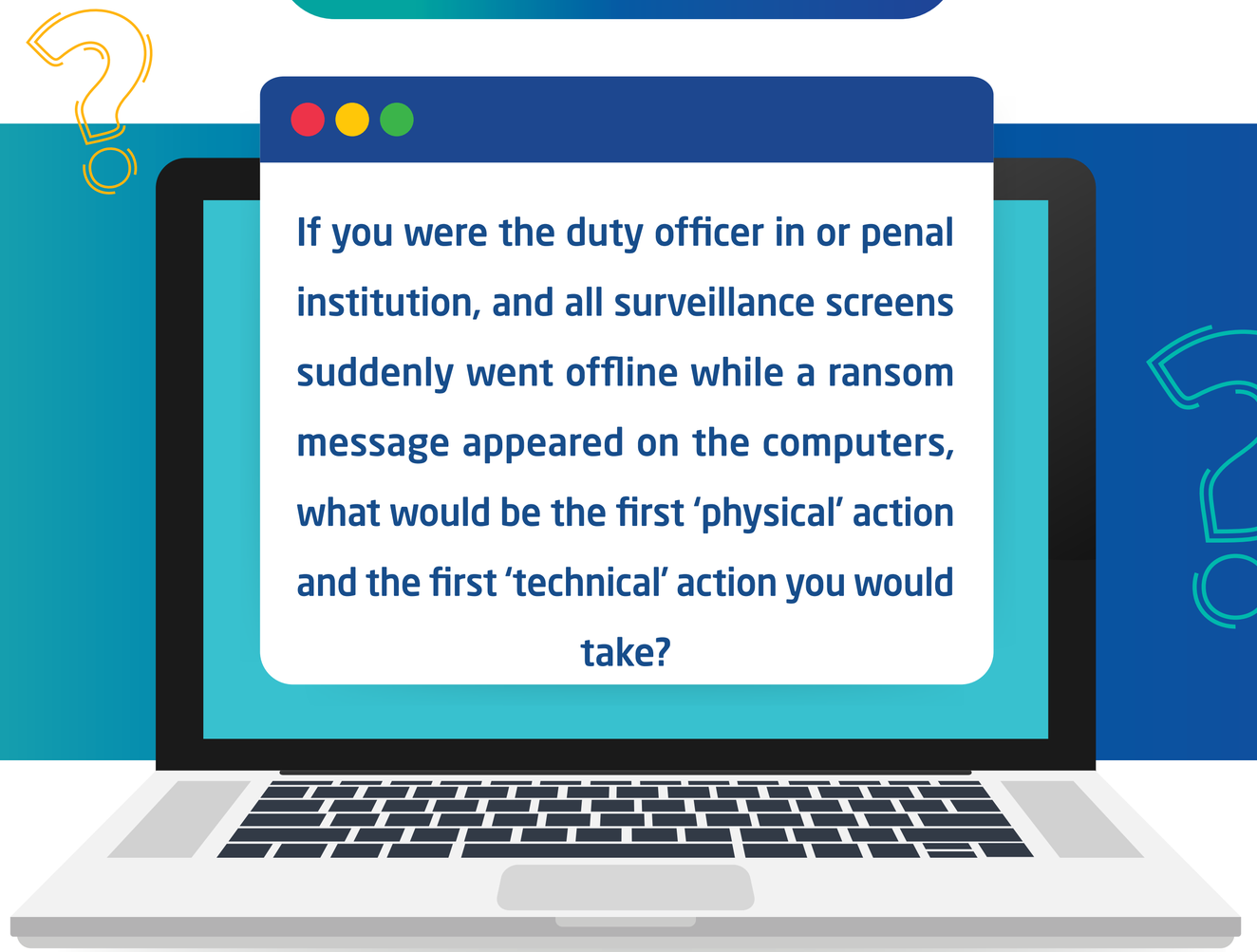
A ransomware attack may disrupt visitation systems, security surveillance systems, and even smart control systems used to manage prisons and correctional institutions, thereby necessitating the declaration of the highest level of security emergency and threatening the safety of both the facility and the inmates.

Statistics

- According to Sophos's 2023 report, 58% of state and local government institutions, including law-related sectors, were affected by ransomware attacks[(1)].
- Average recovery costs following a ransomware attack in the government sector exceed $1.5 million[(2)].

1. Sophos. (2023). The state of ransomware in state and local government 2023. On site: https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-state-and-local-government-2023
2. Sophos. (2024). The state of ransomware 2024. On site: https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

Interactive Question



If you were the duty officer in or penal institution, and all surveillance screens suddenly went offline while a ransom message appeared on the computers, what would be the first ‘physical’ action and the first ‘technical’ action you would take?

Insider Threats

Penal and correctional institutions are particularly vulnerable to cyberattacks due to limited digital awareness or failure to comply with institutional cybersecurity measures.

For example, an employee may use a weak password, such as 123456, or share their password with a colleague, making it easier for their account to be compromised.

Common Insider Threat Vulnerabilities:

01 Lack of effective audit and tracking logs recording who opened each file or document and when, making it difficult to detect suspicious or unauthorised activity within the system.

02 Using external storage devices, such as USB drives, without prior security scanning, as such devices may introduce malware or be used to transfer sensitive data outside the institution in an uncontrolled manner.

Compromising Internet of Things (IoT) Systems

Attackers exploit vulnerabilities in camera software to breach the network.

The Nightmare Scenario

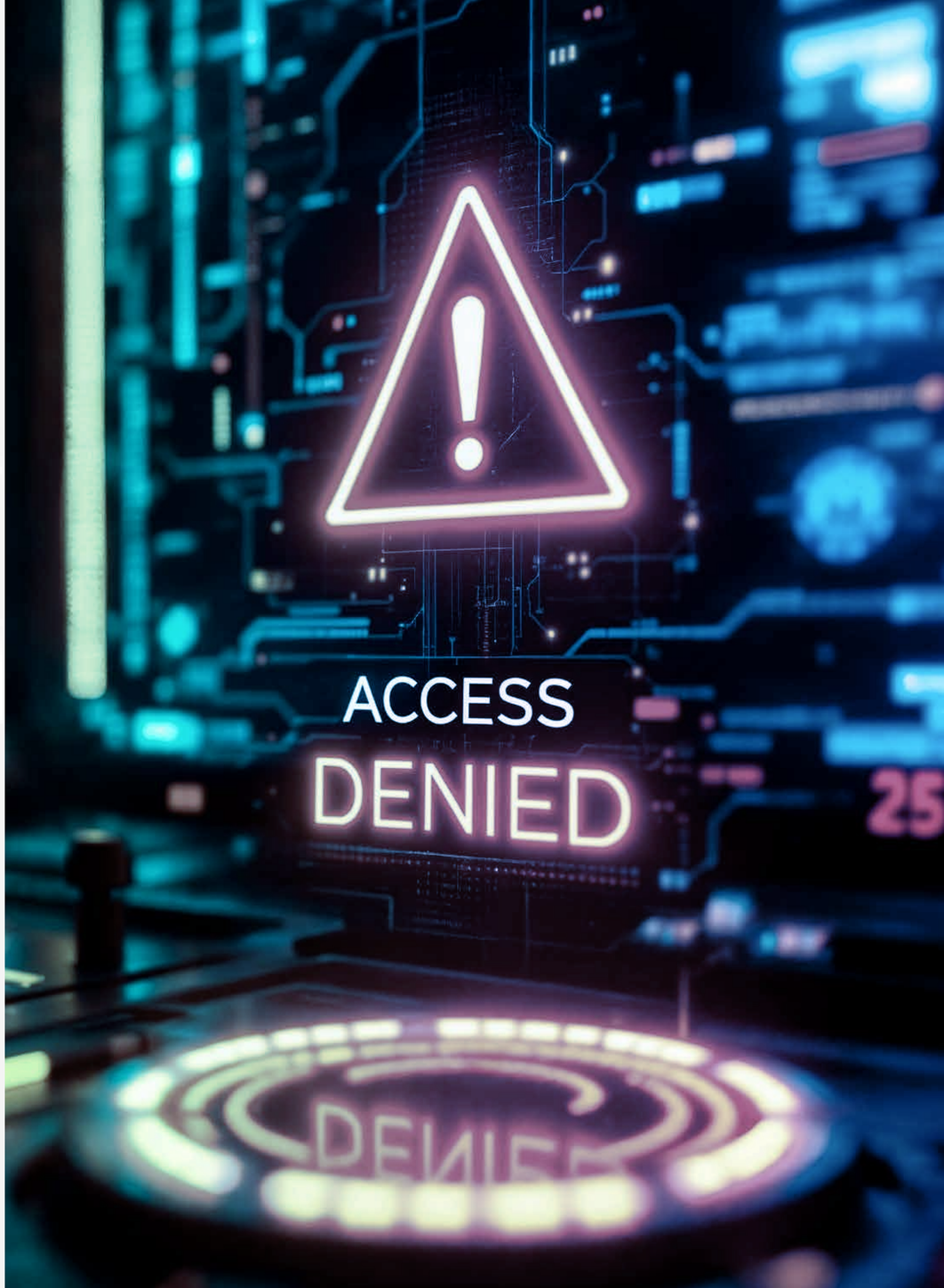
Compromising the camera system and replacing the live feed with previously recorded footage ('looping footage') to conceal unlawful activity or an escape.

Tampering with Electronic Monitoring Bracelets

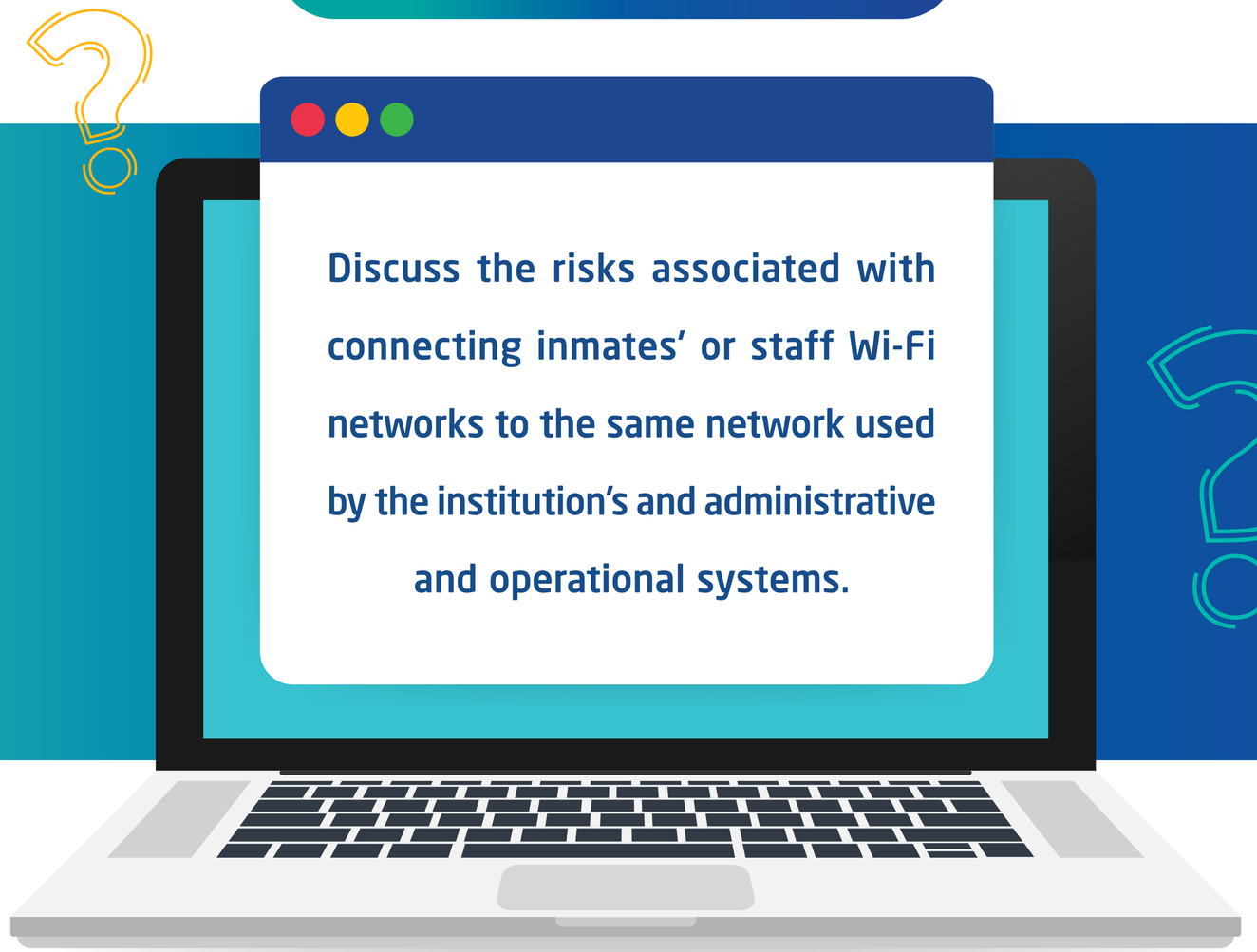
Compromising the GPS tracking system used for individuals under police supervision in order to make it appear that they are at home when they are in fact elsewhere.

Technical Vulnerabilities

- Failure to change the default passwords of cameras and sensors.
- Connecting security device networks to the same network linked to the public internet without isolation.
- Failure to update device software and apply security patches.



Interactive Question



Discuss the risks associated with connecting inmates' or staff Wi-Fi networks to the same network used by the institution's and administrative and operational systems.

Sensitive Data Leakage

The leak may occur either through an external breach of databases or as a result of human error, such as sending a file by mistake or losing an unencrypted computer.

01

Impact on Cases

Disclosing details of an investigation may lead to accomplices fleeing or witnesses being threatened

02

Extortion

Using inmates' or public figures' medical or psychological data to extort them

03

Legal Liability

Exposing the institution to significant legal claims for breach of privacy.

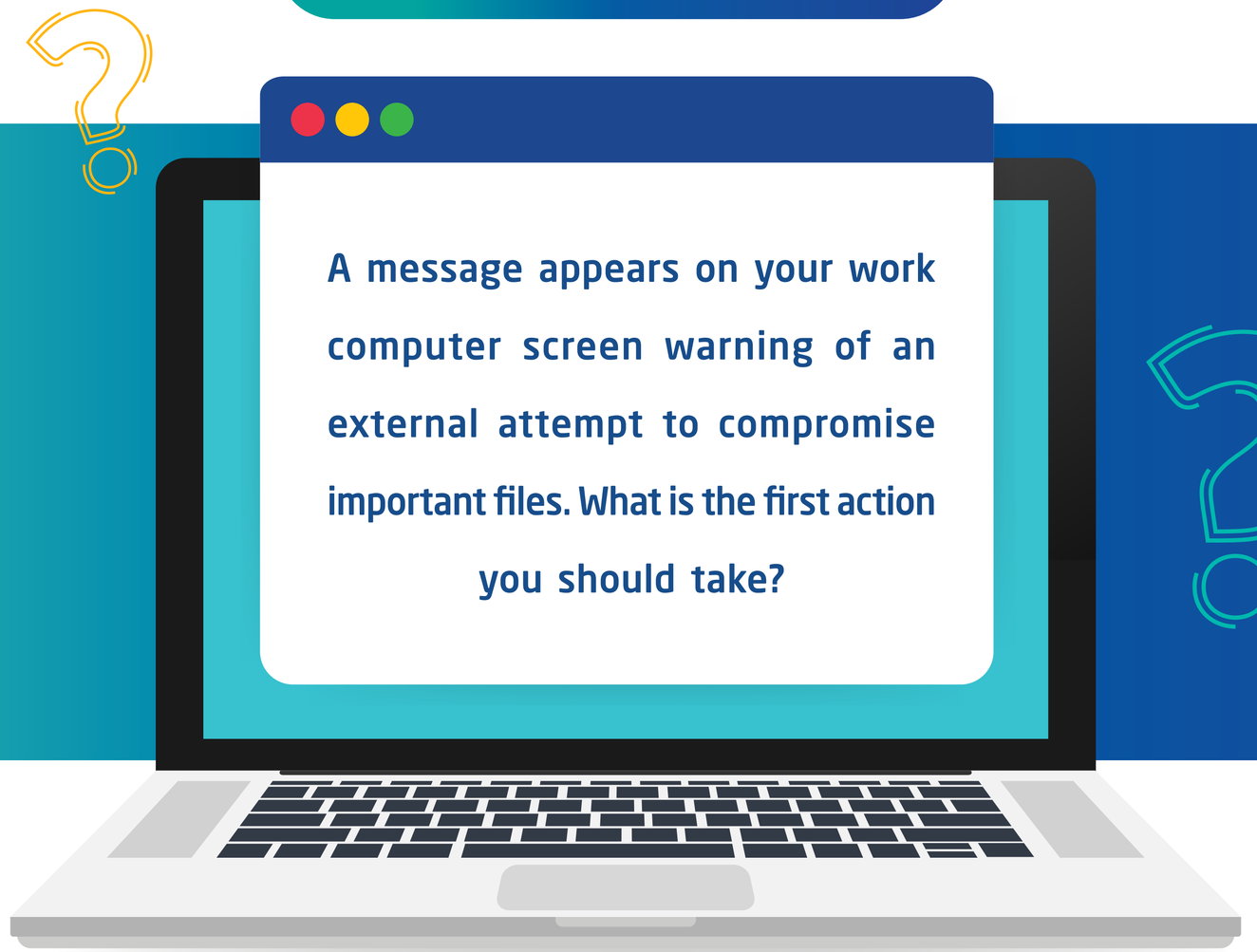
Types of Data Targeted

01 Investigation records, including reports and evidence.

02 Biometric identity data, including fingerprints and iris scans.

03 Records of inmates' visits and communications.

Interactive Question



A message appears on your work computer screen warning of an external attempt to compromise important files. What is the first action you should take?

Focus Area Three

Digital Safety and Prevention Practices

Identity and Access Management (IAM)

Multi-Factor Authentication (MFA/2FA)

Requiring a password together with a code sent to a mobile phone or a biometric identifier, such as a fingerprint, to access sensitive systems. This prevents 99% of account compromise attempts.

Biometric Authentication

Using a handprint or facial recognition to access server rooms or highly sensitive case files.

Regular Review of Access Privileges

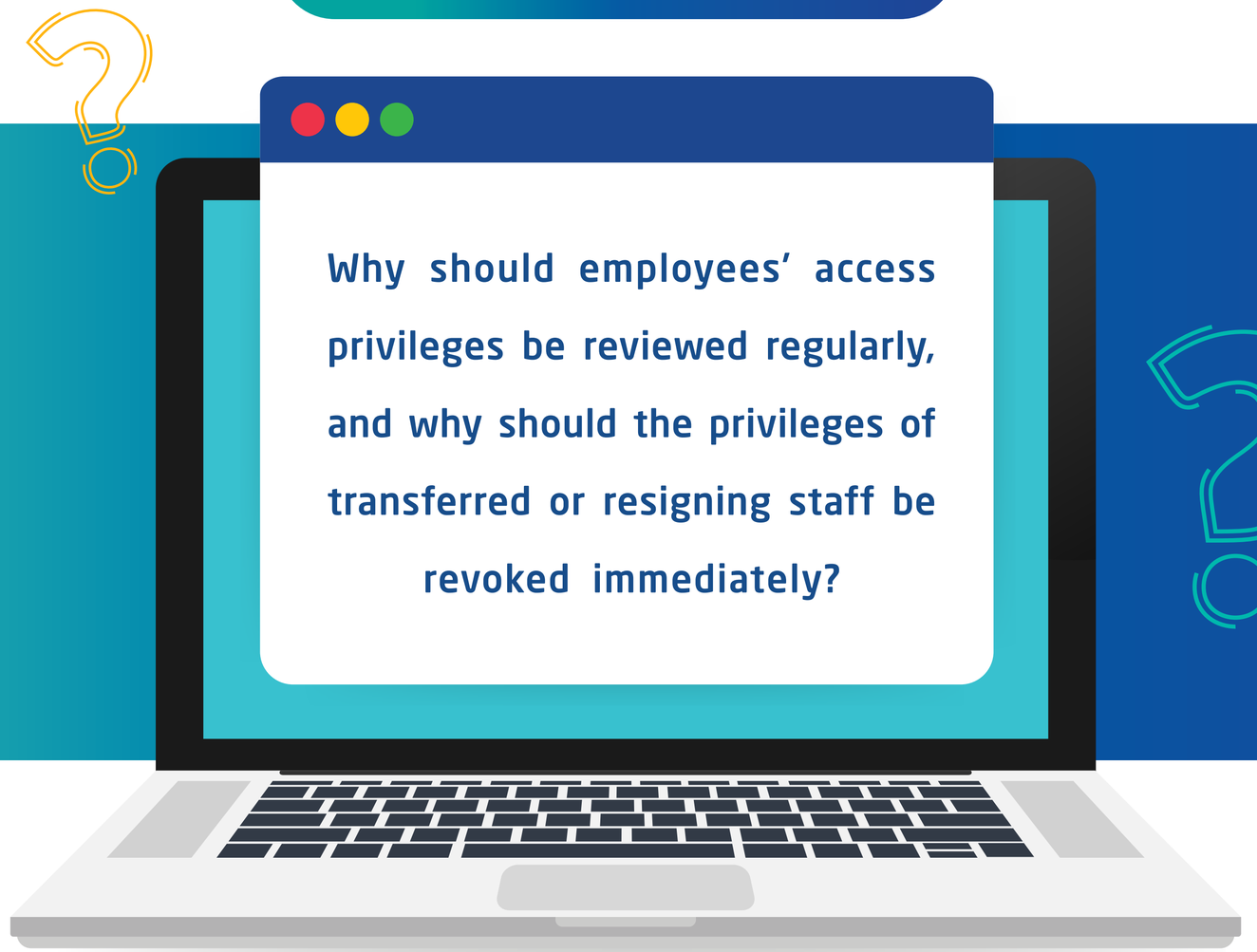
Revoking employees' access privileges immediately upon transfer or resignation to prevent 'orphaned accounts' from being exploited.

Best Practices

Using hardware security keys for prosecutors and heads of penal and correctional institutions rather than SMS codes, which are vulnerable to interception.

Single Sign-On (SSO) with Strict Access Controls.

Interactive Question



Why should employees' access privileges be reviewed regularly, and why should the privileges of transferred or resigning staff be revoked immediately?

Network Segmentation and Digital Isolation

01 Demilitarised Zone (DMZ)

An intermediary network that separates the internet from the institution's internal network and hosts services that must be accessible to external parties, such as the public prosecution's electronic services portal, without granting them direct access to the institution's sensitive internal systems.

02 Isolating Networks for Specific Users

Where educational devices or computers are provided for inmates, they must be placed on a completely separate network with no connection to the public internet or the administrative network, in order to protect data and critical systems.

03 Security System Isolation

Camera networks and door-control devices must operate within a closed network (intranet) and may connect to the internet only through highly secure, encrypted channels such as a VPN.

Importance of the Measure

This measure helps limit the spread of ransomware. For example, if a secretary's computer in the public prosecution is infected with malware, the infection will not spread to the primary database server if the two are separated by network segmentation and a firewall.

Interactive Question

Discuss the risks that may arise if the Wi-Fi network designated for inmates is combined with the network used to transmit confidential investigation data, and explain how network segmentation can mitigate those risks.

Encryption and Backup

01

Encryption in Transit

- Any email or file exchanged between the public prosecution, the police, and the correctional institution must be transmitted through encrypted channels, such as VPN or SSL.

02

Encryption at Rest

- Encrypting the hard drives of laptops and servers. Even if the device is stolen, the thief will not be able to read the data.

03

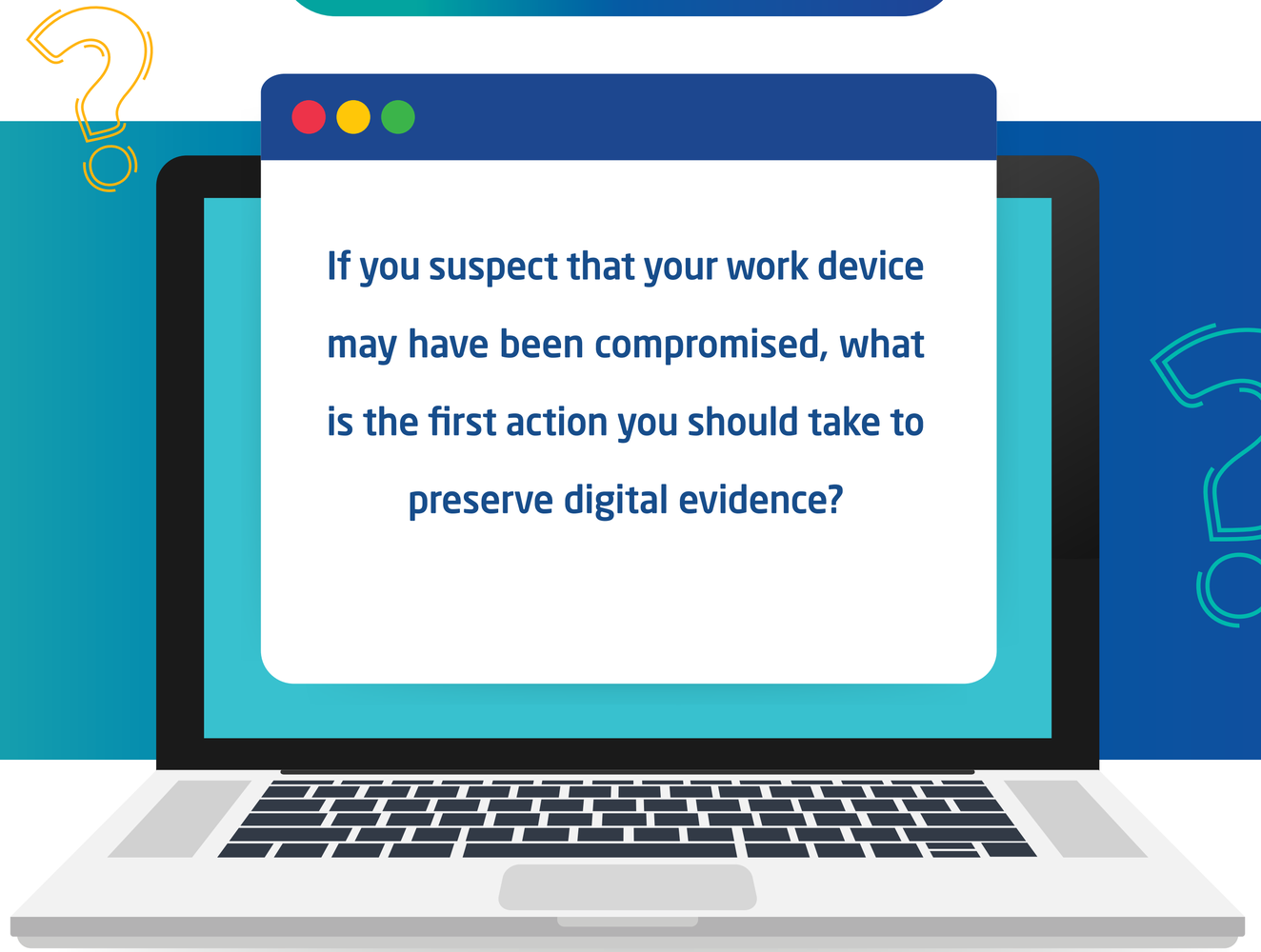
The 3-2-1 Backup Strategy

- Creating three copies of the data
- Storing them on two different media, one in the cloud and one on-premises
- Keeping one copy offline in a geographically separate location to protect it from ransomware and natural disasters.

Digital Evidence

Using hashing to verify that digital evidence, such as videos and documents, remains untampered with from the moment it is seized until it is presented in court.

Interactive Question



Incident Response and Digital Forensic Investigation

01 Computer Security Incident Response Team (CSIRT)

Designating an emergency team comprising technical, legal, and media personnel, and clearly defining their roles.

02 Containment

The first step when an attack is detected is to isolate the affected device from the network to prevent further spread, rather than shutting it down, as doing so may erase evidence stored in RAM.

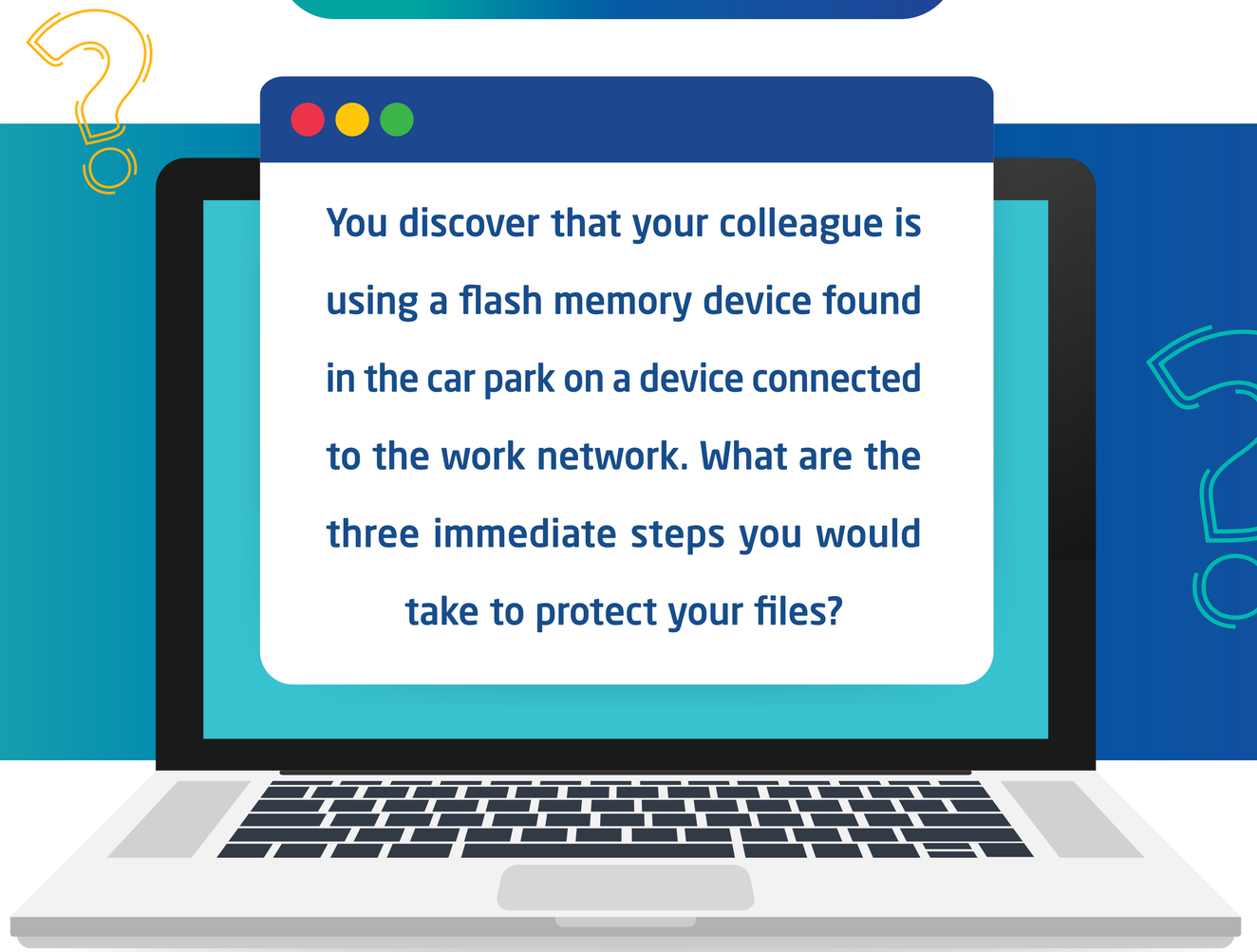
03 Digital Forensics

Preserving the digital evidence of the attack in order to identify the perpetrator and present it as legal evidence against them. This requires leaving affected devices untouched until the specialists arrive.

Handling Protocol

Every employee should prepare a ‘cyber emergency contact list’, as early reporting can help prevent a significant number of cybercrimes.

Interactive Question



You discover that your colleague is using a flash memory device found in the car park on a device connected to the work network. What are the three immediate steps you would take to protect your files?

Cybersecurity Culture

Realistic Simulation-Based Training

01

Conducting simulated phishing campaigns to assess employees' level of awareness and identify those who may require additional training.

Clean Desk and Locked Screen Policy

02

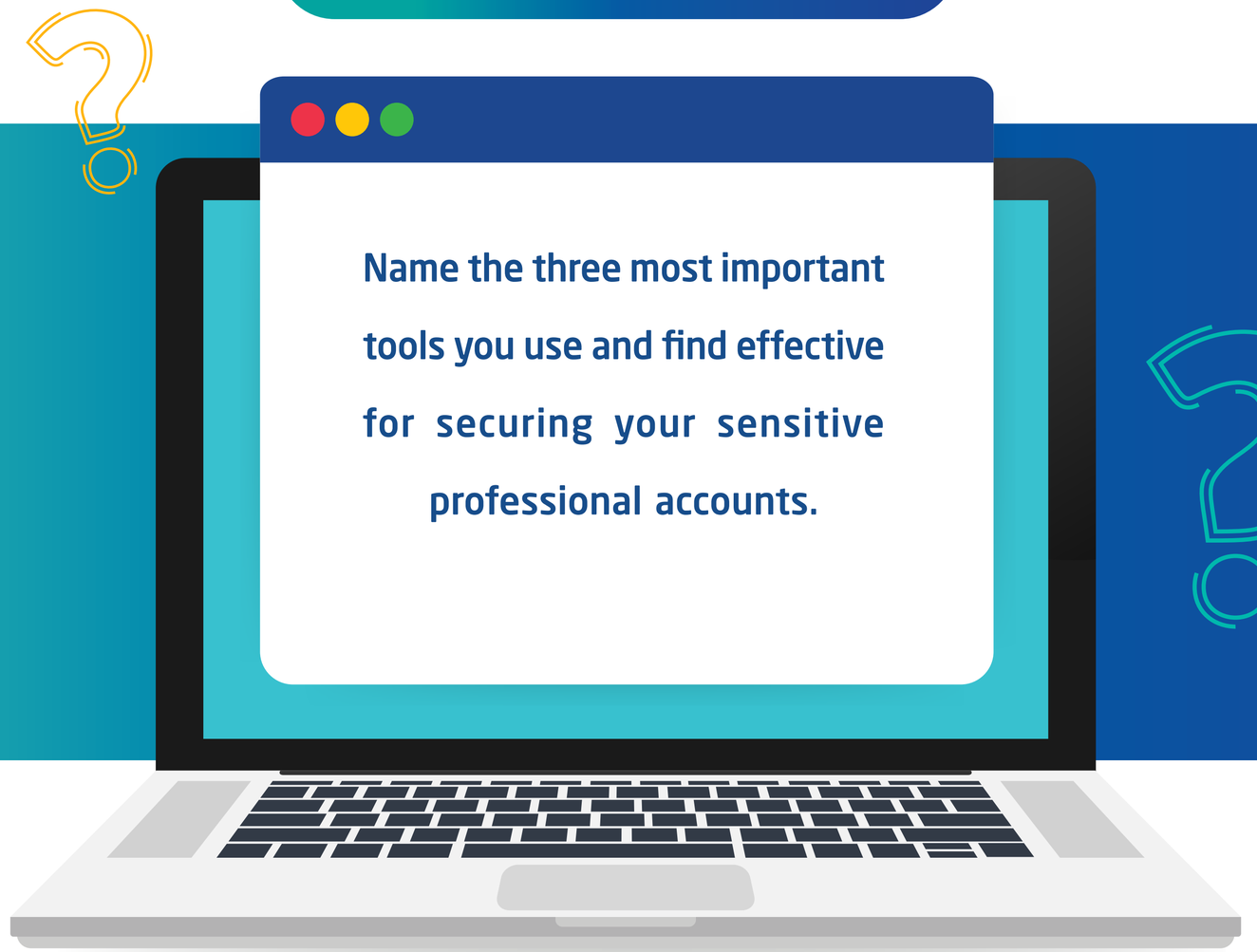
Training employees not to leave sensitive papers on desks and to lock their computer screens whenever they step away, even briefly.

Awareness of Personal Cyber Risks

03

Raising employees' awareness of how to protect their personal devices and bank accounts, thereby improving their security practices in the workplace.

Interactive Question



Vulnerability and Patch Management

1. Immediate Update Policy

Implementing an automated system to scan for vulnerabilities and install critical security updates within 48 hours of their release, particularly for internet-connected systems.

2. Source Code Review

For systems developed specifically for the public prosecution or penal and correctional institutions, the source code must undergo security testing before deployment to ensure that it is free from backdoors.

Information

60% of successful breaches in the public sector exploited vulnerabilities for which a patch was already available but had not been applied.

Securing Communication Channels and Remote Working

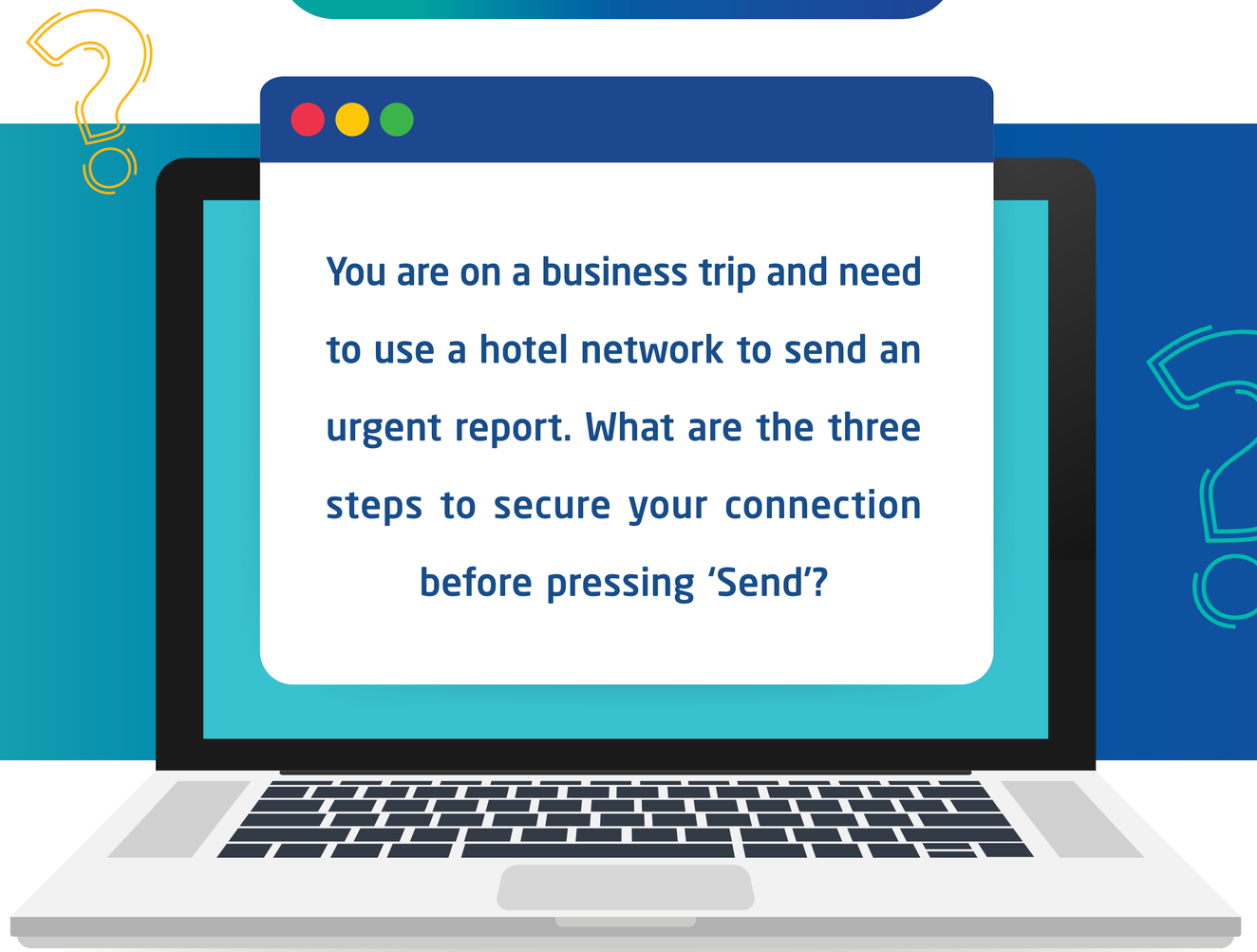
1. Using virtual private networks (VPNs) with strong encryption.

Access central systems only through an approved encrypted VPN, and avoid unsecured public Wi-Fi networks in cafés or airports.

2. Video Conferencing Security

- Meeting rooms must be secured with a unique password for each session.
- The ‘Waiting Room’ feature must be enabled to verify participants’ identities before they are admitted.
- Unauthorised session recording must be prohibited.

Interactive Question



You are on a business trip and need to use a hotel network to send an urgent report. What are the three steps to secure your connection before pressing ‘Send’?

Physical Protection and Port Security

USB Port Blocking

USB ports on all sensitive network devices must be disabled through software controls, or secured with USB port locks to prevent the insertion of any unauthorised storage device.

Secure Charging Points

Employees' phones must not be charged through computer USB ports, whether on work devices or public devices, in order to prevent malware transfer or data theft.

Screen Lock Policy

Paper case files and storage media must not be left on desks, and screens must lock automatically after two minutes of inactivity.

Incident Response and Digital Forensic Investigation

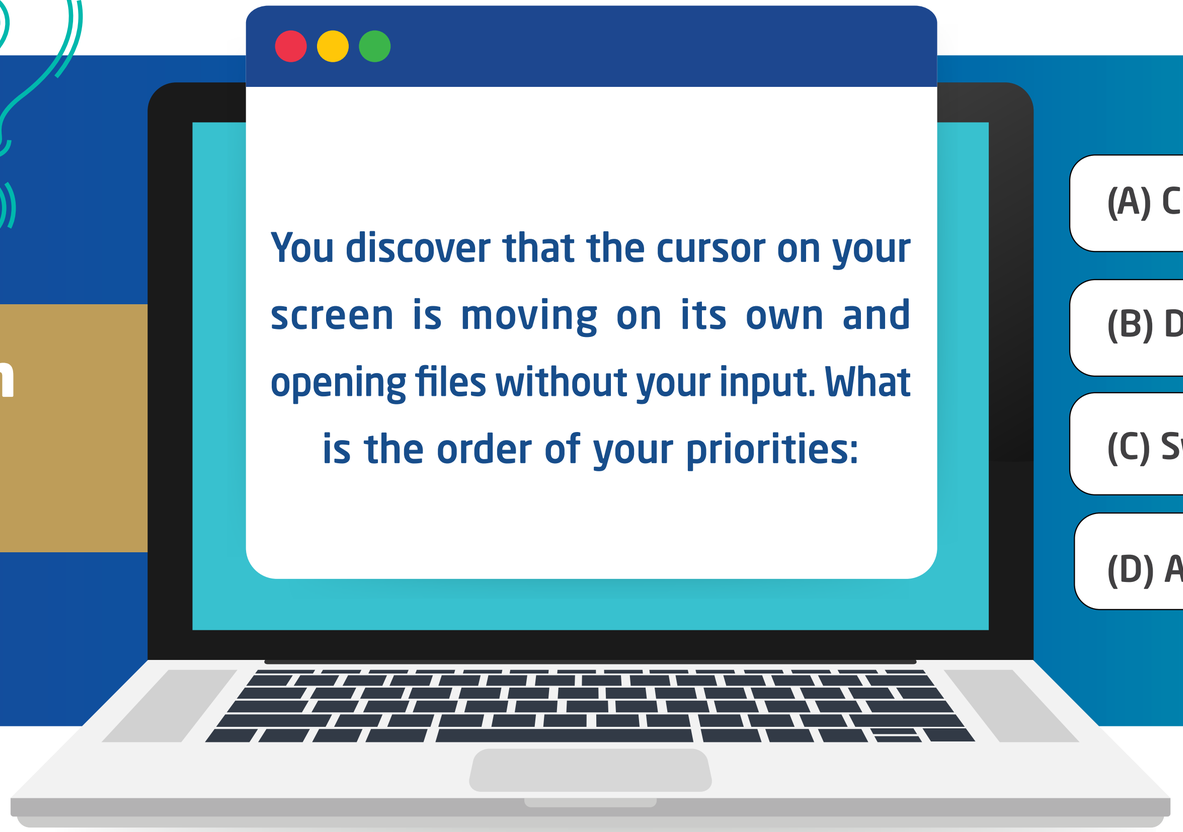
01 Incident Response Plan (IR Plan) through the following phases:

1. **Preparation:** Preparing tools and teams
2. **Detection and Analysis:** Identifying the type and scope of the attack
3. **Containment:** Isolating affected systems by disconnecting the network cable rather than switching off the device
4. **Eradication:** Removing malware
5. **Recovery: Restoring data and verifying that it is free from compromise**
6. **Lessons Learned:** Preparing a report to improve future defences

02 Evidence Preservation

Any attempt by non-specialists to recover files may destroy the digital forensic evidence (‘Digital Footprints’) required to convict the attacker.

Simulation Exercise



You discover that the cursor on your screen is moving on its own and opening files without your input. What is the order of your priorities:

(A) Contact your manager

(B) Disconnect the internet cable

(C) Switch off the computer

(D) Attempt to deal with the attacker yourself.

References

1. Casey, Eoghan. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press. (A bible for Digital Forensics in Prosecution). Online: https://rishikeshpansare.wordpress.com/wp-content/uploads/201602//digital-evidence-and-computer-crime-third-edition.pdf

2. Cybersecurity Challenges for Federal Attorneys and Judges. Online: https://www.fedbar.org/blog/cybersecurity-challenges-for-federal-attorneys-and-judges/

3. Jewkes, Yvonne & Reisdorf, B. (2016). Tough on Crime, Tough on Technology? The 'Smart' Prison and the Future of Corrections. Stirling University. (Specifically covers the IoT and technology risks in prisons). Online: https://www.researchgate.net/publication/304574547_A_brave_new_world_The_problems_and_opportunities_presented_by_new_media_technologies_in_prisons

4. Veronika Hofinger and Philipp PflegerI. A reality check on the digitalisation of prisons: Assessing the opportunities and risks of providing digital technologies for prisoners. Online: https://www.researchgate.net/publication/379052768_A_reality_check_on_the_digitalisation_of_prisons_Assessing_the_opportunities_and_risks_of_providing_digital_technologies_for_prisoners

5. ENISA (European Union Agency for Cybersecurity): Threat Landscape Report. Online: https://www.enisa.europa.eu/

6. National Center for State Courts (NCSC). (2021). Cybersecurity Basics for Courts and Justice Systems. Online: https://www.ncsc.org/resources-courts/cybersecurity-basics-courts

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Contact The National Cyber Security Academy

16555 - 40466379 - 51045944

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