الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Data Security and Digital Safety

Target Segment

Media Professionals

Teacher's Guide

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Data Security and Digital Safety

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

1655

00974 404 66 798

00974 510 45 944

academy@ncsa.gov.qa

Table of Contents	Page

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 specifically designed to serve as an educational resource for media professionals, covering digital safety principles, best practices their devices and data during field coverage. It also aims to teach them how to safely use public networks and protect images and other journalistic sources.

Moreover, this resource provides effective strategies on how to protect online reputation and manage digital identity, making digital safety a daily professional priority for media professionals.

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

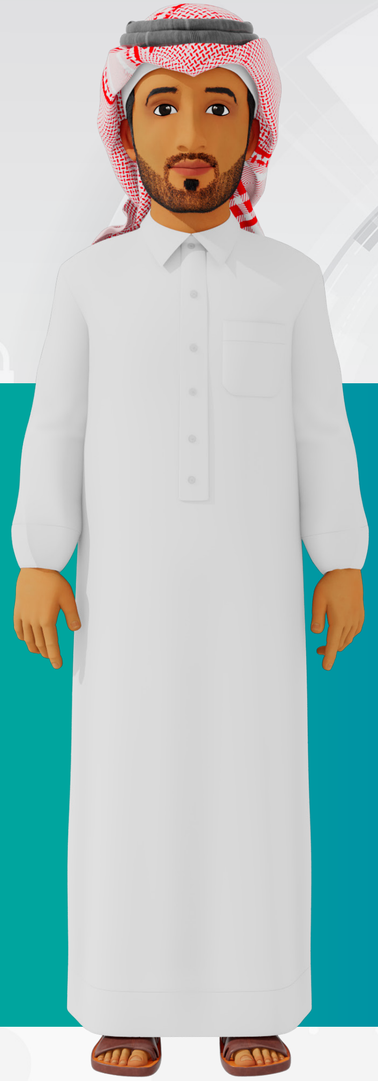
Digital Safety National Initiative

About the Initiative

This initiative encompasses a series of awareness activities on digital safety and cybersecurity, aimed at the local community across all age groups, social demographics, and professional sectors.

It was launched to promote awareness about digital safety and the safe use of the internet and various technological applications. Providing a detailed outline on the potential risks of cyberattacks, this booklet aims to build a cyber-secure and technologically empowered society.

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

Chapter One

Data Security During Field Coverage

Protection of Devices while Traveling

Mobile devices are indispensable for fieldwork, yet they remain the most vulnerable to loss or theft.

Protection Steps

- Use strong passwords and full encryption for mobile devices
- Carrying computers and phones in safe bags with locks
- Disable auto-connecting to Wi-Fi or Bluetooth networks while commuting
- Enable the Find My Device feature; it can be locked remotely when it is lost

Managing Sensitive Data in Investigative Journalism

Investigative journalism frequently handles sensitive information that demands rigorous protection.

Safety Management Steps

Classify data according to its sensitivity level: Normal, Confidential, or Highly Confidential.

Use unique passwords for highly important files

Store sensitive files on encrypted drives or storage devices

Avoid copying data to unprotected external media

Safety Procedures When Using Public Networks

Public Internet networks are more vulnerable to cyber-attacks.

Protection Steps

- Avoid accessing sensitive accounts or data over a public internet network
- Usie a VPN to protect data traffic
- Enable personal firewall when connecting to public networks
- Log out of all accounts immediately after use

Benefits of Using VPNs

VPNs are among the most effective tools for securing your internet connection.

Benefits of Using VPNs

- Encrypting data traffic and prevent its interception
- Changing the device's online address to hide the user's location
- Reducing hacking risks when using public networks

Data Protection

Protecting data is a cybersecurity priority; therefore, it is essential to follow specific steps to prevent its leakage or destruction.

Protection Measures

- Archive final materials in secured servers
- Delete unnecessary files to prevent leakage
- Transfer sensitive files to offline storage media
- Conduct regular reviews to ensure data remains secure and over the long term.

Dealing with Anonymous Online Sources

Anonymous sources can provide valuable information, yet they may also be exploited as a means to mislead journalists.

Prevention Measures

Use email or account-tracking tools to verify the sender's authenticity

Confirm Digital Identity

Use encrypted messaging apps when secure communication is required

Interaction through secure channels

It is the process of comparing information against multiple reliable sources

Cross-verification

Protecting Images and Videos

photos and videos gathered by journalists may contain sensitive evidence or field details that could be exploited against them or their sources.

Protection Measures

Use secure storage media

such as encrypted disks or cloud storage

Grant limited access

Share materials only with trusted parties

Use watermarks

Preserve rights and establish source attribution when republishing

First Interactive Question

1 **What is the major risk of using the public Internet without protection tools?**

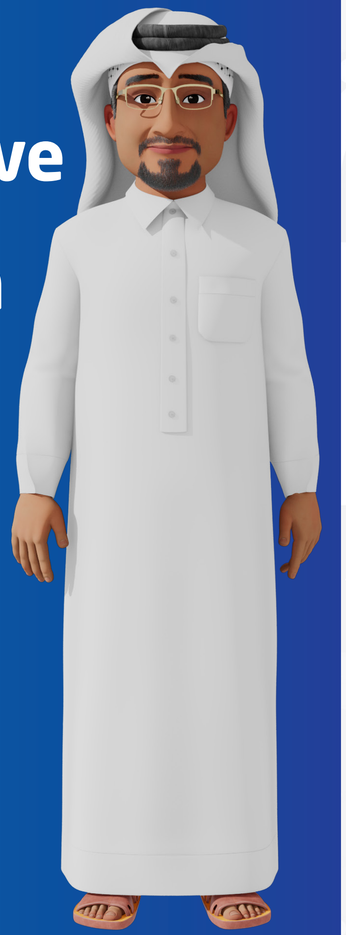
- **A.** | Slow internet speed
- **B.** | Risk of data interception and unauthorized account access
- **C.** | Reduce the size of sent files.
- **D.** | Difficulty logging into accounts

Second Interactive Question

2 What is the primary purpose of using VPN during field coverage?

- **A.** | Increase internet speed
- **B.** | Improve video quality
- **C.** | Encrypt connections and hide the real location
- **D.** | Store large files on the server

Third Interactive Question



3 **Why is it recommended to delete unnecessary files after completing an investigation?**

- **A.** | Only to speed up device performance
- **B.** | To provide more storage capacity
- **C.** | To reduce the likelihood of data being leaked or exploited
- **D.** | To increase internet speed

Chapter Two

Digital Safety for Journalists and Media Professionals

Managing Digital Identity

A journalist's digital identity is the virtual reflection of their personality and credibility.

Safety Management Steps

- Maintain clear separation between personal and professional accounts
- Regularly review security settings for social media accounts
- Use only official images and names in professional accounts
- Monitor and report immediately any digital identity plagiarism or forgery

Electronic Reputation Protection

Online defamation can be weaponized to target and undermine journalists.

PROTECTIONISM MEASURES

Enable alerts to track online mentions of your name or organization.

Communicate with platforms to quickly remove abusive content

Respond with caution and steer clear of public arguments that amplify negative spread

Strategies for Dealing with Breach Attempts

Digital attacks may target devices, accounts, or even entire press organizations.

Response Steps

Immediately isolate the affected device or account from the network

Identifying the type of attack (phishing, hacking, malware...)

Change passwords for all linked accounts

Report to the technical team/ organization for urgent action.

Using Cybersecurity Tools

Some tools enable journalists to significantly strengthen their digital defenses.

Key Tools

- Advanced antivirus software with automatic update features
- Personal firewalls to prevent intrusion and hacking
- Strong file encryption and password protection tools
- Password manager software

Privacy on Social Media Platforms

Digital privacy is the journalist's first line of defense, as it helps reduce the chances of being targeted or having information gathered about them.

Important steps to protect your privacy

Review app permissions regularly

Disable any unnecessary permissions, such as access to your camera or contacts

Manage friends and followers' lists

Accept friend requests from trusted people only and review suspicious accounts periodically

Restrict post visibility

Use privacy settings to control who can see content

Monitor fake accounts

Continuously search for accounts impersonating the journalist and report them

Social Engineering

Social engineering is among the most dangerous hacking methods, as it targets journalists' psychology and behavior more than their devices.

Protection Measures

Avoid sharing passwords

Passwords are personal and must never be shared with anyone, regardless of their perceived trustworthiness

Verify caller's identity

Verify phone numbers and emails before responding to any sensitive request

Be cautious of calls or messages claiming to be from official entities

Verify through official channels and avoid immediate responses

Follow the principle of professional skepticism

Treat any unexpected communication with caution until proven otherwise.

Fourth Interactive Question

4 **What is the primary objective of managing a journalist's digital identity?**

A. | Increase the number of followers

B. | Enhance credibility and protect accounts from impersonation

C. | Improve internet speed

D. | Reduce battery consumption

Fifth Interactive Question

5 **What is the first step to take when discovering a device breach?**

- **A.** | Continue using the device
- **B.** | Simply restart the device
- **C.** | Immediately isolate the device or account from the network
- **D.** | Delete all files

Answers to Interactive Questions

01 **Answer to first interactive question**

b. Potential data interception and account access

02 **Answer to second interactive question**

c. Encrypt connections and hide the real location

03 **Answer to third interactive question**

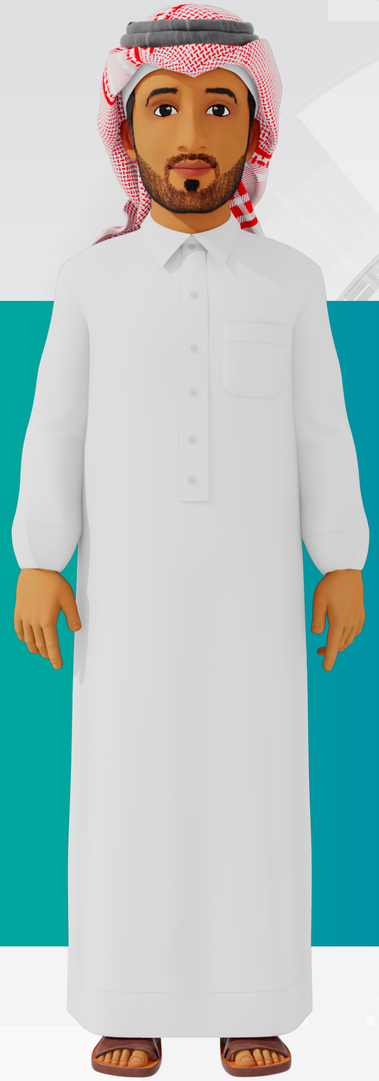
c. To reduce the likelihood of data leakage or exploitation

04 **Answer to fourth interactive question**

b. Enhance credibility and protect accounts from impersonation

05 **Answer to fifth interactive question**

c. Immediately isolate the device or account from the network



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