الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Protecting Devices and Verifying Information Sources

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

Protecting Devices and Verifying Information Sources

Target Segment

Media Professionals

Teacher's Guide


Email or username
****
Remember Me
Forgot Password?
LOGIN
REGISTER

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 - 40466798 - 51045944

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

Table of Contents	Page No.

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 for device protection, and information source verification. It aims to equip them with the best practices to assist them in securing their devices and personal and business data. It also teaches them how to safeguard their devices against hacking attempts and data loss by applying encryption, backup strategies, and two-factor authentication.

The booklet also focuses on strengthening media professionals' capacity to counter digital disinformation by verifying images and videos, detecting deepfakes, and addressing misleading content.

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.

Digital Safety National Initiative

About the Initiative

This initiative covers a collection of awareness activities in the field of digital safety and cybersecurity targeting the local community across different age groups, social segments, and professional sectors.

It was launched to promote awareness about digital safety and the secure use of the internet and various technological applications, highlighting the potential risks, with the goal of building a cyber-secure and technologically empowered society.

Target Segments

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

- People with Special Needs
- Women and Family
- Senior Citizens
- Financial and Banking Sector
- Civil Society Organizations
- Expatriate Workers
- University Students

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

Chapter One

Protecting Devices and Verifying Information Sources

Protecting Computers and Mobile Phones

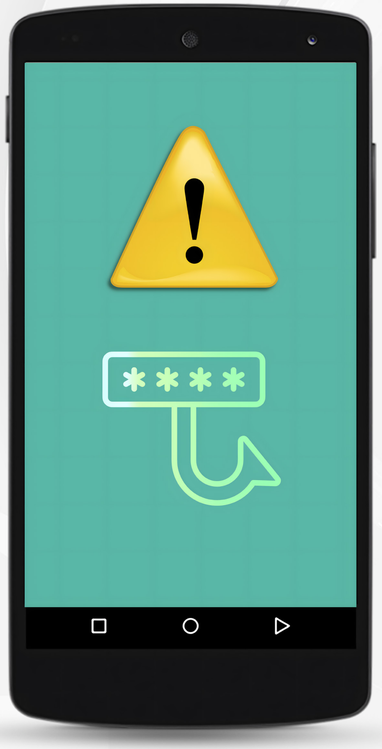
For journalists, digital devices are essential to their work and any compromise of these gadgets poses a direct threat to the safety of their information sources. It should therefore be treated as the first line of defence.

Protection Steps

- Lock the device using a strong password or fingerprint to reduce the possibility of unauthorised access
- Ensure that operating system and software are regularly updated to avoid exploitation of security vulnerabilities
- Install a protection software (antivirus + firewall) to prevent most hacking attempts
- Disabling of Bluetooth and Wi-Fi when they aren't in use reduces the chances of hidden infiltration into the device

How can a mobile phone get hacked?

Hacking occurs when an unauthorised person accesses the phone or its contents without the knowledge of its owner.



Common Methods of Phone Hacking

- Downloading fake apps containing malware
- Clicking on fraudulent links attached with email messages or on websites
- Connecting to unsecured Wi-Fi networks
- Sharing login credentials or passwords with strangers
- Losing a phone without a password

Regular Software Updates

Updates are not just improvements. Rather, they often provide solutions to serious vulnerabilities that hackers may exploit.

Benefits of Updates

Enabling automatic updates helps prevent delays in applying critical security patches

Applications including editing software require regular updates to maintain stability and optimal performance

Delaying software updates means leaving the door open for cybercriminals

Encryption and document protection

Encryption is an essential step to protect your data as it keeps files confidential even if they are stolen.

Advantages

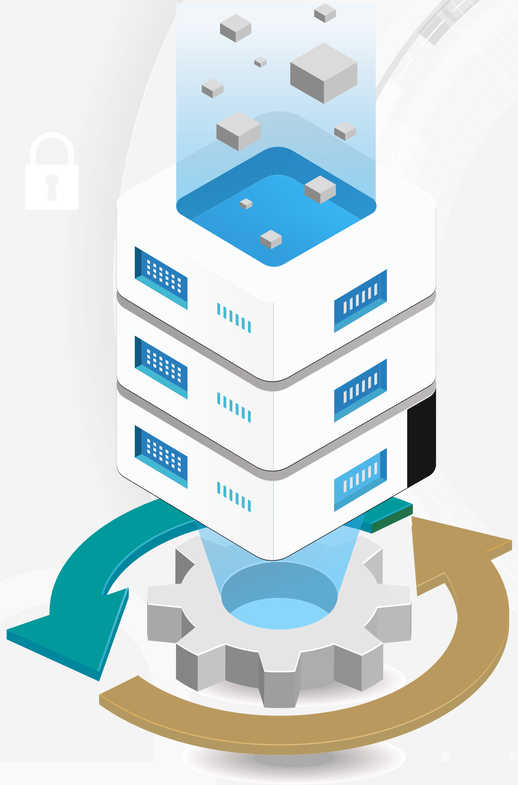
Full hard disk encryption prevents data access when devices are lost

Assigning a distinct password to highly sensitive documents adds an extra layer of protection and strengthens overall security

Using tools like BitLocker to secure investigative reporting files

Data backup

File loss can result from cyberattacks or technical failures, and data backup is the only guarantee for recovery.



Best Practices

- Store a copy in cloud storage for easy access from anywhere
- Follow a regular schedule (weekly or monthly) to ensure new file updates aren’t lost
- Create an additional copy on an offline external drive to avoid ransomware encryption

Two-factor authentication (2FA)

Adding an extra layer of security increases the difficulty for hackers to gain unauthorized access.

This is achieved by entering a one -time code, either sent to your phone or generated via a dedicated application after you have entered your password

Advantages

This means hackers would need access to your personal device, not just your password

This security measure is available on most platforms and email

Private Wi-Fi Network Security

The internet is your device's gateway to the outside world, and any vulnerability can become an entry point for attacks.

Security Steps

Changing the network's default password intercepts simple intrusion attempts

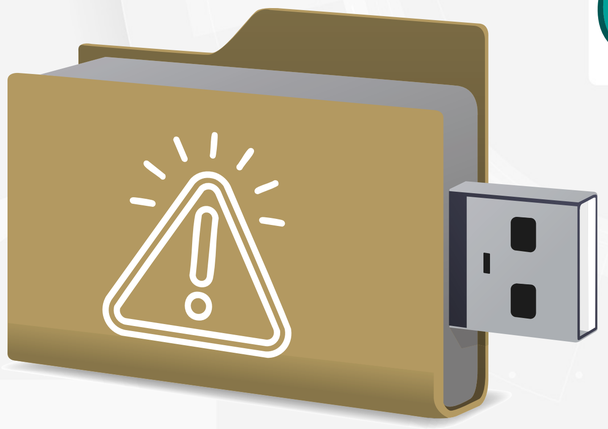
Enabling WPA2 or WPA3 encryption adds advanced-level protection

Regularly reviewing connected devices reveals any unauthorized access

Storage Media Protection

Hard drives and USB storage devices are essential tools, and the information they contain should be safeguarded.

Methods of Protection



- Encrypt files before transferring them to a USB or external drive keeps them confidential
- Scanning any external storage device before accessing its contents helps prevent viruses from spreading to computers or other devices.
- Avoiding the use of untrusted disks and drives lowers the risk of malware infection.

Signs of Device Breach

Early detection of breach signs helps reduce potential losses.

Key Warning Signs

A sudden slowdown in device performance, despite minimal active programs, may signal malicious software running in the background

The appearance of unfamiliar files or the disappearance of existing ones is a strong sign of abnormal activity

Applications or messages launching without user action may indicate external system control

Data Recovery After Breach

If an attack succeeds, certain actions can help reduce its impact.

Steps

- Disconnect the device from the internet to halt any data leakage
- Using backups to quickly recover files
- Recourse to reconfiguration (Format); if protection solutions do not work

First Interactive Question

1- What is the safest way to backup files?

a	Save them to offline external disk.
b	leaving it on the desktop.
c	Storing it on a USB drive that remains permanently connected to a device.
d	Send by e-mail

Second Interactive Question

2- What is the most prominent indicator that a device is infected with malware?

a	Device overheating and slowing down despite running few programs.
b	Sudden increase in internet speed.
c	Applications closing after finishing with them.
d	System updates are installed automatically.

Third Interactive Question

3- What is the primary objective of two-factor authentication?

a	Speed up the login process.
b	Make the account requires two different steps to confirm access.
c	Store data in the cloud
d	Completely eliminate passwords

Chapter Two

Verifying Information Sources and Countering Disinformation

Concept of disinformation

Disinformation refers to media content that is produced or disseminated with the intent to deceive, cause confusion, or influence public opinion. It can be written, visual, or audio content.

It may be entirely fabricated and bear no relation to reality.

May be based on real facts taken out of their context

Key Characteristics of Disinformation

Often involve exaggerating numbers or events

Frequently mention vague or unknown sources

Verifying Images and Videos

Images and videos rank among the most heavily exploited assets in disinformation, particularly with the advent of advanced editing technologies.

Verification Methods

Use reverse image search to determine its origin and date

Examine shadows or location features for consistency with the reported event

Use reliable tools to analyse videos and detect frames and details

Cross-reference content with multiple trusted sources

Deepfakes and Fabricated Videos

Deepfakes have emerged as one of the most dangerous tools of disinformation, owing to the difficulty of detecting them.

Detection Indicators

- Mismatched lip movement with sound in videos
- Unnatural visual details such as colors or shadows
- Lack of verifiable original sources or initial dissemination via unverified channels.
- A video is limited to a single version despite its supposed importance

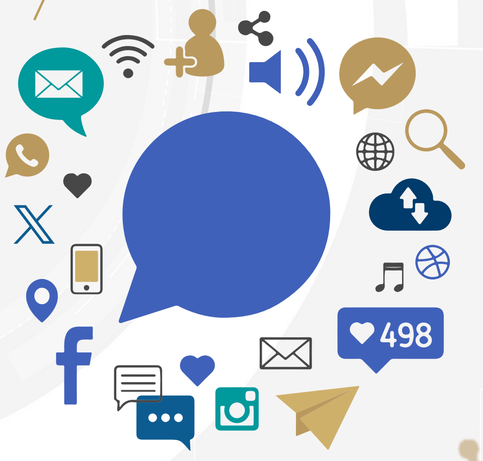
Social media as a tool for spreading disinformation

Social media has accelerated circulation of false news at an unprecedented rate.

Key Characteristics of Social Media Posting

Using attention-grabbing headlines to drive engagement without fact-checking the content

Rapid reposting of news without prior verification



Using edited images and hashtags to spread rumors

Using “trending” as false proof of credibility

Steps to Prevent Falling Victim to Disinformation

To reduce the risk of falling victim to disinformation, there are several essential preventive measures.

Prevention Steps

- Avoid rushing to share any news before fact-checking them
- Rely on multiple and diverse sources before accepting information
- Build a network of trusted sources to confirm news
- Raising public awareness about the dangers of disinformation and detection methods

Warning signs of misleading content

Disinformation frequently exhibits repetitive linguistic patterns that can be spotted.

Warning Signs

- Using exaggerated emotional language to provoke fear or anger
- Relying on phrases like “informed “sources” or “ unnamed expert
- No precise details such as location and time
- Exaggerating numbers and statistics without authenticated sources

Cyberattacks Related to Disinformation Circulation

Disinformation campaigns often begin with attempts to compromise journalists' accounts or media institutions.

Signs of such attacks

- Email hacking to publish fake news under the journalist's name
- Taking control of social media accounts to spread rumors
- Targeting media websites with denial-of-service attacks to disable them
- Using malware to spy on devices and steal information

Protecting accounts against breach

Journalists' digital accounts are an essential gateway to misleading attacks.

Protection Steps

- Use strong and unique passwords for each account
- Enabling two-factor authentication for additional protection
- Review recent activities on your accounts to detect any unauthorised access
- Be cautious of suspicious emails or links

Fourth Interactive Question

4. What is the primary objective of disinformation?

a	Reporting facts as they are
b	Misleading the public or influencing the public opinion.
c	Rapidly spreading false news

Fifth Interactive Question

5. What is the most prominent indicator that a video is fabricated using deepfake technology?

a	High image resolution
b	Automatic system updates
c	Unnatural details appearing in faces, colors, or shadows
d	Multiple versions of the clip available from different sources

Sixth Interactive Question

6. What are the consequences of clicking an unknown link in an email message?

a	Improving internet connection speed
b	Automatic system updates installation
c	Redirecting the user to fake pages or downloading malicious software
d	Increasing device storage capacity

Answers to Interactive Questions

01 **Answer to first interactive question**

a. Store it on an offline external drive

02 **Answer to second interactive question**

a. Device overheating and slowing down despite few running programs

03 **Answer to third interactive question**

b. Make the account require two different steps to confirm access

04 **Answer to fourth interactive question**

b. Misleading the public or manipulating the public opinion

05 **Answer to fifth interactive question**

c. Inconsistencies in facial features, colors or shadows

06 **Answer to sixth interactive question**

c. Redirecting the user to fake pages or downloading malicious software

Prior to concluding: Please take a moment to fill out your personal information and evaluate the workshop.
Scan the QR code below.

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency