مكتب أبوظبي الإعلامي
Abu Dhabi Media Office

دائرة التمكين الحكومي
DEPARTMENT OF GOVERNMENT ENABLEMENT

ADCMC
مركز إدارة الطوارئ والأزمات والكوارث لإمارة أبوظبي
Emergencies, Crises and Disasters Management Centre Abu Dhabi

حملة مجتمعنا جاهز

OUR COMMUNITY IS PREPARED

Guidelines for Cybersecurity Awareness During Emergencies

Be vigilant and be part of protecting your country and your family

Content

Click the title to be directed to its page

01 Objective

This guide aims to **enhance public awareness of cybersecurity risks** and promote safe digital practices, enabling individuals to protect their personal data and online accounts when using various digital services, particularly during crises and exceptional circumstances, thereby reducing exposure to cyber threats and avoiding victimization.

02

Importance of **Raising Cybersecurity** Awareness Among Community Members

Adhering to safe digital practices contributes to:

Supporting national digital security

Protecting individuals' digital privacy across all segments of society

Safeguarding personal and financial data from breaches

Securing digital accounts from unauthorized access

Reducing the risk of online fraud

Limiting the spread of cybercrime

03

Concept of **Cyberattacks**

Cyberattacks are attempts that target individuals or entities to:

Stealing data

Compromising accounts

Disrupting digital services

Spreading misinformation

Impersonating identities

Exploiting users through fraudulent methods

04

Reasons for the Increase in Cyberattacks **During Crises**

Cyberattacks tend to rise during crises due to:

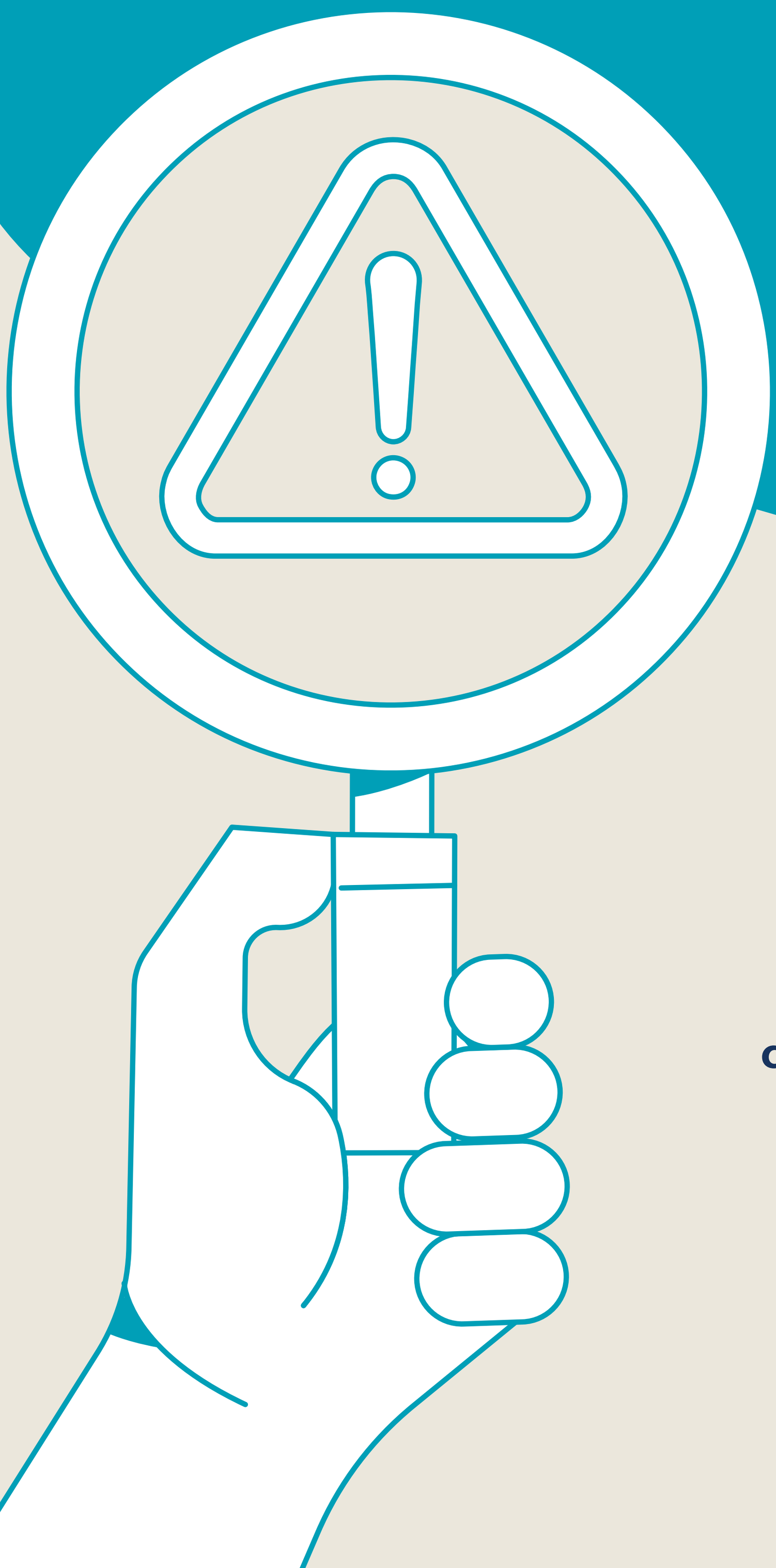
Exploiting fear and confusion among individuals, making them easier to deceive

Rushed digital decision-making without adequate verification

Weak information verification, alongside the spread of rumors and unconfirmed news

Increased reliance on unofficial channels for obtaining information or services

05 Common Cybersecurity **Threats**



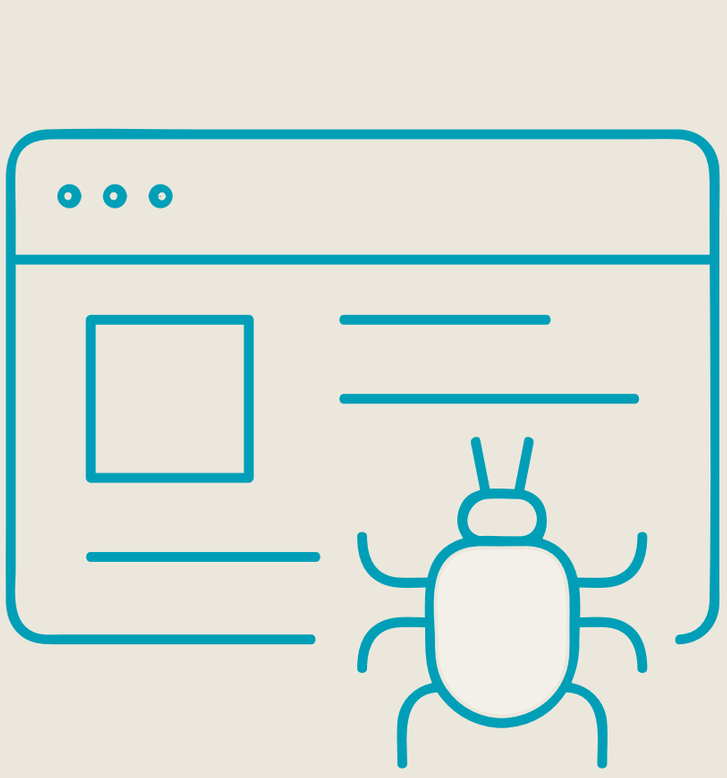
The most common cyber threats include:

Phishing and online scams

Emails, text messages, or calls containing fake offers that impersonate official or trusted entities, aiming to trick you into clicking malicious links, sharing personal or banking information, or transferring money through unofficial channels.

Account compromise

It often occurs due to the use of weak or repeated passwords, or because of sharing login credentials with others.

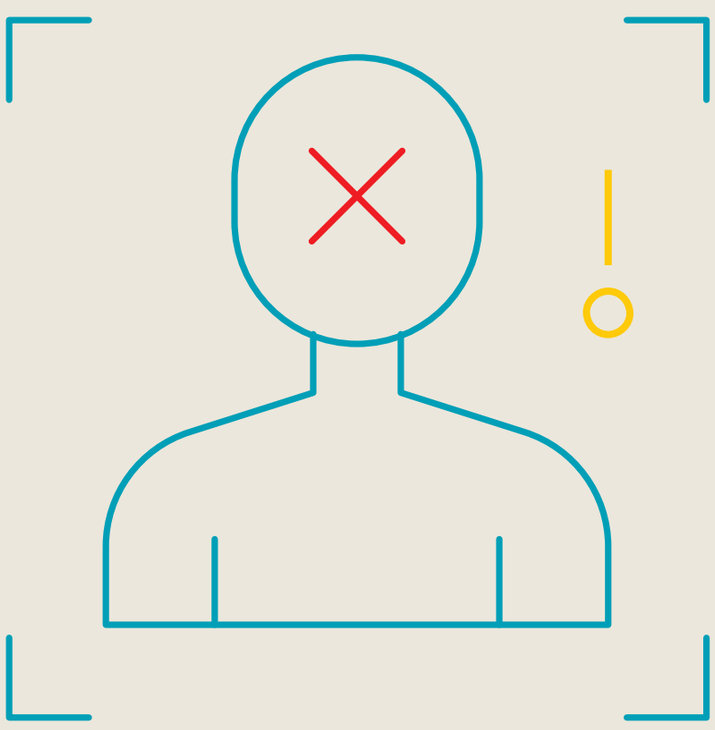


Malware

Harmful programs or files installed by clicking suspicious links or opening attachments from unknown sources.

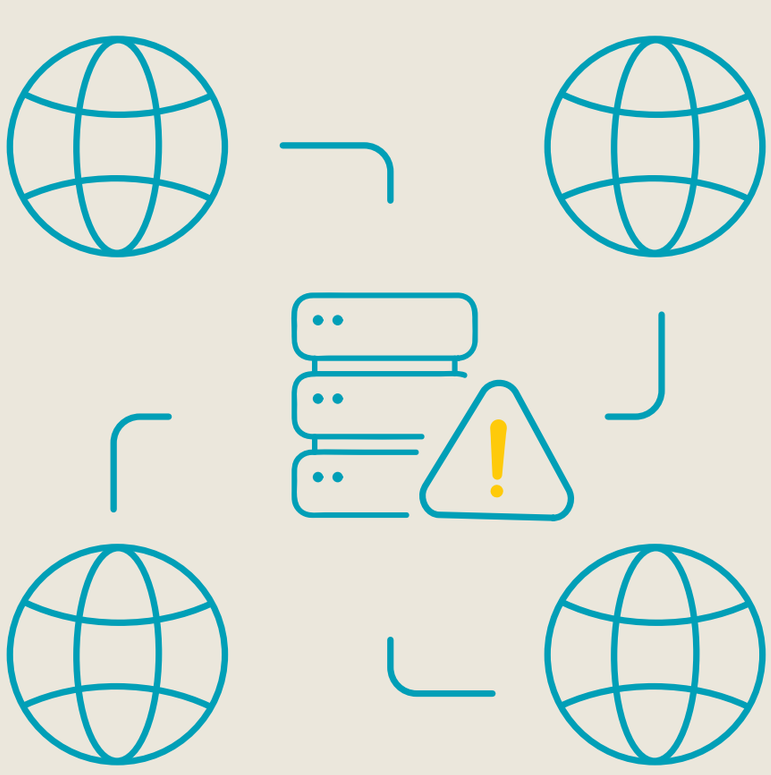
Impersonation and fake social media accounts

Using your personal data or photos or creating fake accounts that impersonate individuals or organizations to commit fraud, mislead others, spread malicious links, or request personal information



AI-enabled fraud and deepfakes

Such as mimicking voices or creating fake images or videos that appear to be from trusted entities or individuals, with the aim of deception or fraud.

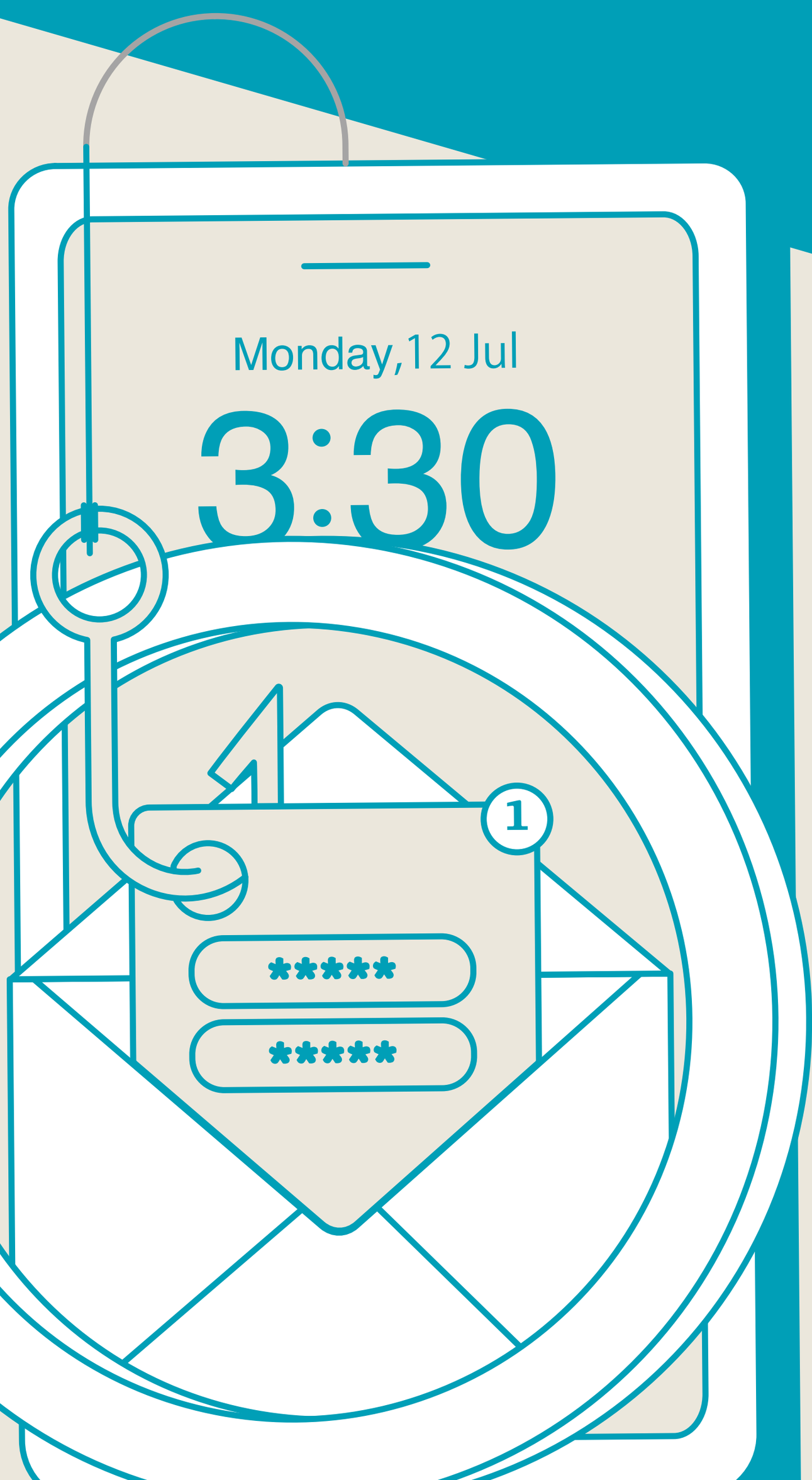


Data leakage through untrusted websites

Occurs when entering personal information or uploading files on unsafe or unknown websites or platforms

06

Indicators of **Suspicious** Messages and Links



Key signs that may indicate a fraud attempt include:

Urgent requests for personal information or verification codes

Links from unknown or untrusted sources

Sudden requests to transfer money

Messages claiming unexpected and valuable prize winnings

Unrealistic offers or discounts

Login notifications from unfamiliar devices

Unexpected voice messages or videos requesting information

Messages written in an unusual tone or overly formal manner

Impersonation of official or trusted entities

07

Common Mistakes **to Avoid**

Key indicators of a potential fraud attempt include:

Clicking on unknown or suspicious links

Using the same or similar passwords across multiple applications

Downloading apps from unofficial websites or sources

Uploading files or entering data on untrusted websites or platforms

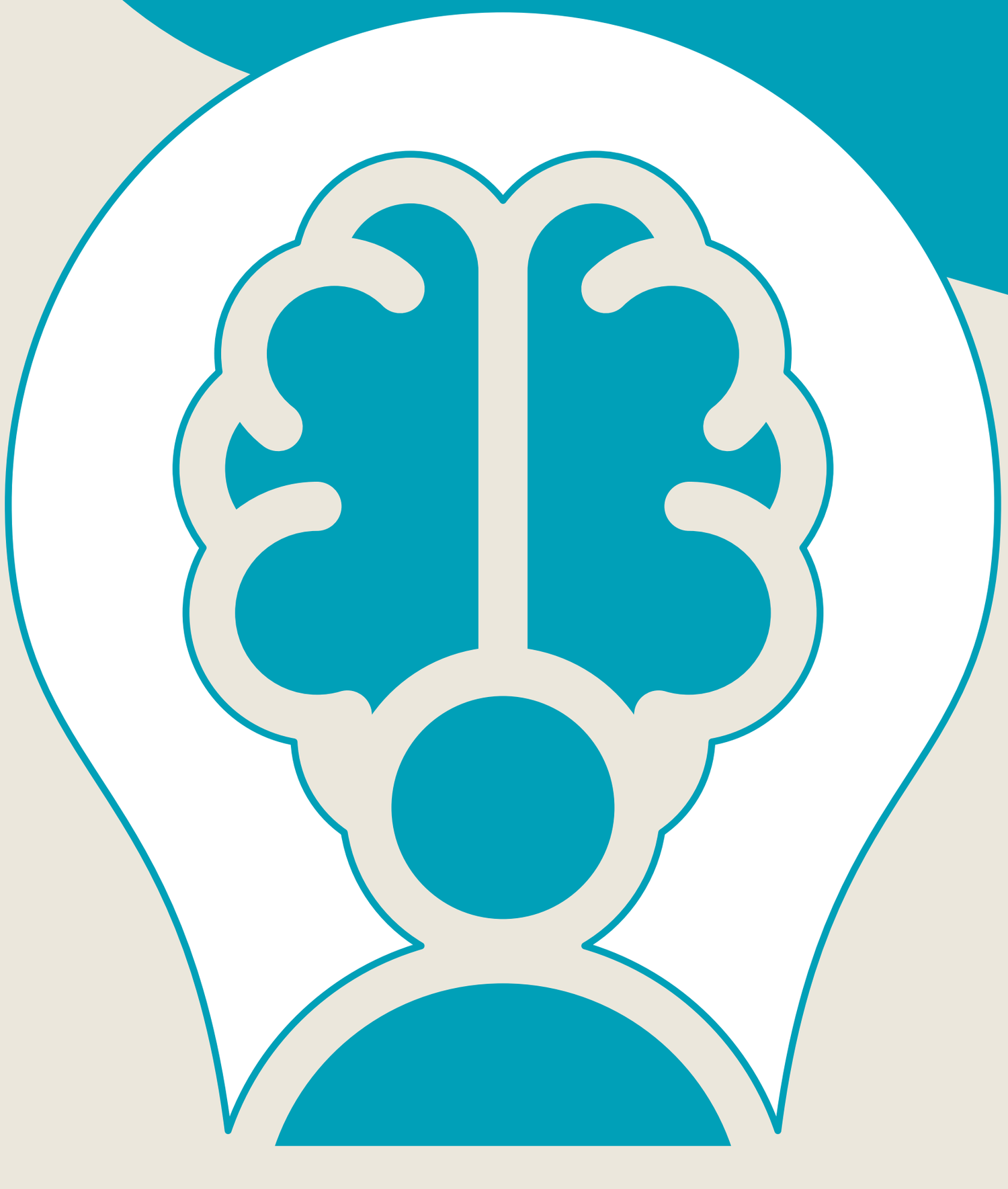
Sharing one-time passwords (OTP) with others

Responding quickly to suspicious messages without verification

Reposting unverified information or media

08

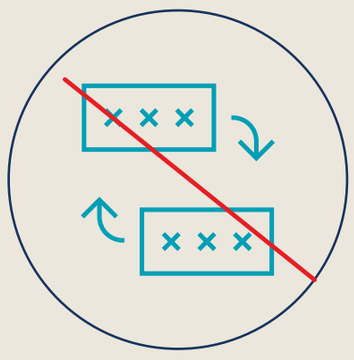
Safe Digital Practices and Protecting Accounts & Personal Data



To maintain your cybersecurity, make sure to:

Use strong passwords containing uppercase and lowercase letters, numbers, and special characters (14 characters or more)

Enable two-factor authentication (2FA) on your accounts



Do not use the same password for more than one account

Verify the legitimacy of any request before sharing personal, banking, or verification information

Confirm the source of messages and links before interacting with them

Download applications only from official and trusted sources

Regularly update your devices and applications

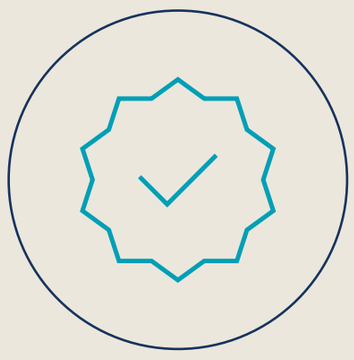
Check the credibility of websites before entering any personal information

09

Safe Digital Behavior During Crises

During crises, you should:

Remember that you are contributing to the protection of our nation

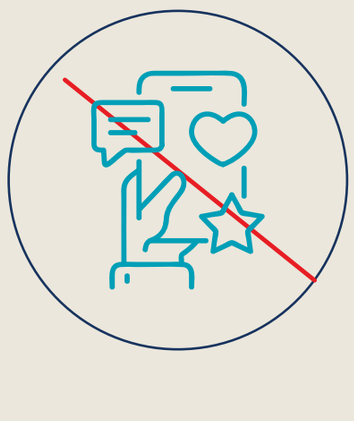


Rely only on official sources

Avoid sharing unverified information

Be cautious of messages that exploit exceptional circumstances

Verify the authenticity of audio or video content before reposting



Avoid reacting impulsively to messages that provoke fear or urgency

Follow the security procedures issued by the relevant authorities

10

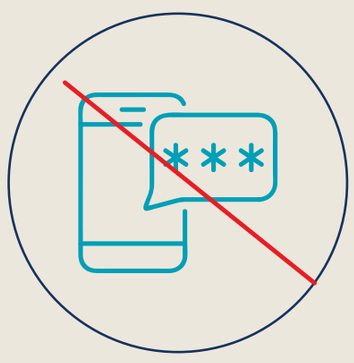
Protecting Children and Seniors Digitally

It is recommended to:

Educate children not to share personal information, such as full name, location, or family details

Verify the apps being downloaded, especially those used for children's games

Inform older adults about common fraud methods, such as calls or messages requesting personal information or money



Never share one-time passwords (OTP) with anyone, even if they claim to be from an official entity

Help them verify messages and links before clicking or interacting with them

Encourage older adults to report immediately if they suspect any unusual message or request

Educate children to follow remote learning guidelines, including using official platforms and not sharing login credentials

Avoid using educational email accounts on public websites or platforms, especially gaming apps, to prevent account compromise or misuse

Our Community is Prepared

Guidelines for Cybersecurity Awareness During Emergencies

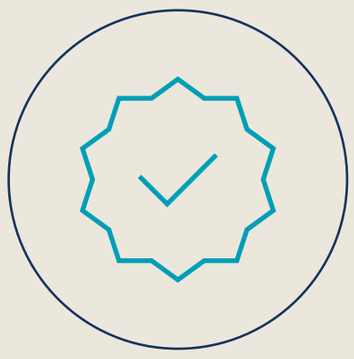
11

Safe Use of Social Media

Safe use can be ensured by:

Adjusting privacy settings

Do not share your real-time location information to avoid putting yourself at risk



Sharing official documents with authorized entities and through official platforms

Be cautious of fake or impersonated accounts

Do not interact with untrusted links or contests that may be used to steal your data

Verifying news or media before reposting to help prevent the spread of rumors

Stay calm and avoid getting drawn into heated discussions to protect yourself from exploitation

12 Emergency **Contact Numbers**

In case of **emergencies or suspected cybercrimes**, please contact the relevant authorities immediately using the following numbers:

Abu Dhabi Police

999

Cybercrimes

Aman Service

8002626

SMS

2828

Use the Cybercrime platform provided by the Ministry of Interior, available on official app stores:

App Store

Google Play

AppGallery

REINFORCING CRISIS READINESS

adcmc_ae

adcmc.gov.ae