الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Audience
Civil Society Organisations

Trainer's Guide

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Digital Safety Principles

Target Group:

Civil Society Organisations

Trainer's Guide

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

January 2025

Doha, Qatar

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Contact the National Cyber Security Academy

00974 404 663 79

00974 404 663 62

www.ncsa.gov.qa/

academy@ncsa.gov.qa

Table of Contents	Page

Introduction

Digital safety is an essential element for ensuring information security and protecting individuals and communities from the increasing threats in Cyberspace.

This booklet has been developed to raise awareness among people with special needs about the principles of digital safety and the best practices that help them avoid cyber threats. It aims to enhance their understanding of key risks, such as phishing, identity theft, and malware, emphasising the importance of making digital safety a vital priority.

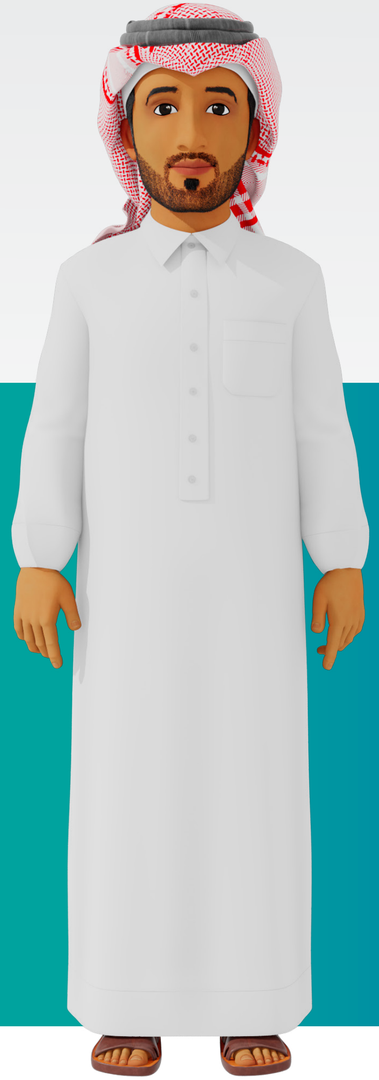
These efforts are part of the National Initiative for Digital Safety, organised by The National Cyber Security Agency, to establish a secure digital environment for all members of society.

About the Initiative

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.

The goal of the initiative is to spread awareness about digital safety and the secure use of the internet and various technological applications, clarifying 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:

- 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

Common Cyber Risks

Online Identity Theft

Online identity theft is one of the most dangerous cybercrimes facing individuals and companies, where millions of people are exposed to the theft of their personal information each year, which is then used illegally for financial or fraudulent purposes.

Reasons for Identity Theft

01 The widespread use of the internet

Increased reliance on the internet has made personal information more vulnerable to theft.

02 Security vulnerabilities

Insufficiently secured websites and applications can lead to data breaches.

03 Lack of security awareness

A lack of awareness of electronic protection methods makes users more vulnerable to cyberattacks.

Facts and Information

Online identity theft costs the global economy more than $50 billion annually.

Identity Theft Tools

Email Identity Theft

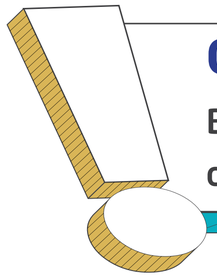
By hacking the victim's email, the hacker can find important personal information, such as bank account numbers and login data for websites, which facilitates the process of identity theft.

Online Shopping Fraud

This involves exploiting a shopping account to make purchases without the victim's knowledge, either through data breaches, phishing, or malware.

Identity Theft of the Elderly and Children

The elderly and children are more vulnerable to identity theft attacks to obtain personal information and access the elderly's bank accounts or take the child's data to create other accounts to defraud others or blackmail the child.



Caution!

Be wary of using weak passwords, such as names or dates that are easy to guess, and always choose complex passwords containing letters, numbers, and symbols.

How Can Online Identity Theft Be Executed?

01

Identity theft is closely linked to phishing and social engineering techniques, which are usually used to extract sensitive personal information from victims.

02

Once this information is collected, cybercriminals begin to take over the victims' bank accounts or carry out legal procedures in their name, such as issuing licenses and concluding contracts.

Types of Ransomwares

Crypto Ransomware

This type encrypts the user's files and requests a ransom to decrypt them.

Locker Ransomware

This type prevents access to the device entirely, not just the files, and requests a ransom to restore access.

Scareware

This relies on intimidation by sending false notifications claiming to have detected malware and requesting a ransom to fix the problem.

Doxware

This threatens to publish sensitive information stolen from the victim if the ransom is not paid.

Cyber Risks Facing Civil Society

1. Theft of Sensitive Data: Civil society organisations store various personal and sensitive information, such as national identities, health records, and financial data, which could be exploited in cyberattacks.
2. Disruption of Public Services: Cyberattacks, such as Distributed Denial of Service (DDoS) attacks, can interrupt essential infrastructure, including water, electricity, and healthcare services.
3. Attacks on Communication Networks: Targeting communication networks may result in the disruption of emergency reporting systems and internal communications.
4. Social Engineering: Attackers employ deceptive messages to manipulate staff into divulging login credentials or granting access to sensitive systems.
5. Reliance on Outdated Technology: Using obsolete software heightens the risk of security vulnerabilities.

Common Cyber Threats

1

Phishing

Attackers use fraudulent emails to deceive employees into revealing sensitive information.

2

Ransomware

Encrypting critical organisational data and demanding a ransom for its decryption.

3

Malware

Malicious software designed to disrupt systems or steal information.

4

DDoS Attacks

Flooding networks with illegitimate requests to disable services.

5

Supply Chain Attacks

Targeting supplier organisations to gain indirect access to core systems.

Impacts of Cyberattacks

1. **Financial Losses:** Expenses related to system repairs, ransom payments, and legal compensations.

2. **Loss of Trust:** Data breaches affecting customers or citizens undermine confidence in the organisation.

3. **Service Interruptions:** Attacks can cause temporary or prolonged paralysis in the delivery of public services.

Impact of Cyberattacks

4

Legal and Regulatory Consequences: Organisations may face legal liabilities and fines for non-compliance with cybersecurity standards.

Damage to Reputation: Cyberattacks tarnish the reputation of civil organisations among the public.

5

Preventive Measures and Security Strategies

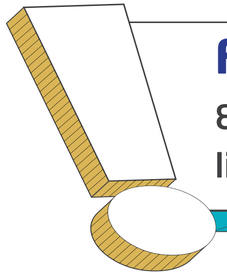
Passwords for Mobile Phone Protection

Passwords are the first line of defence for mobile phones. When creating passwords, consider the following:

- Choose a combination of characters, numbers, and symbols.
- Avoid using the same password for multiple accounts or devices.
- Change passwords regularly.

Biometric measures, such as fingerprint or facial recognition, provide an additional layer of security to protect mobile phones and their data from intrusion or theft in case of loss.

However, it is recommended to enable a backup password or PIN in case biometric authentication fails or is compromised.



Facts and Information

85% of cyber security breaches are due to errors made by internet users, such as opening unknown links, providing personal data to strangers, or not following safe internet browsing instructions.

Biometrics for Mobile Phone Protection

Biometrics provide an additional layer of protection for mobile devices and include:

- Fingerprint recognition.
- Facial recognition.
- To enhance security, it is recommended to enable a backup password or PIN in case biometric authentication fails or is compromised.

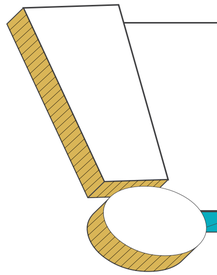
Encrypting Mobile Phone Data

Encryption is the process of converting data into unreadable code that can only be accessed by authorised parties using an encryption key.

Mobile phone storage space and application data can be encrypted.

Encrypting mobile phone data is an effective tool for protecting important data from theft in case the device is hacked, stolen, or lost.

The encryption process converts data into unreadable and incomprehensible code, preventing attackers from exploiting it.



Facts and Information

Financial Losses resulting from cyberattacks are increasing significantly and are expected to exceed $10 trillion in 2025.

Methods of Encrypting Mobile Phone Data

Encryption can be activated on iOS devices from the settings menu by selecting 'Face ID & Passcode', which will prompt the user to enter their screen lock code, then scroll to the bottom of the page where the phrase 'Data Protection Enabled' will appear.

Android devices can be encrypted by selecting the 'Security' field from the settings, then selecting the 'Encryption' option, and finally choosing 'Encrypt Phone'.

If the phone is not charged or the encryption process is interrupted, all data will be lost, as the encryption process takes around an hour or more. Therefore, it is important to be well-prepared before starting the process.

Digital Identity Security and Communication Security

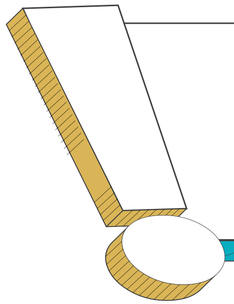
Protecting digital identity from theft depends on ensuring a secure internet connection, which can be achieved through the following:

01

When entering personal information online, ensure the connection is secure. It is always recommended to use a home network or cellular data and avoid public Wi-Fi networks, which are unprotected.

02

Use a VPN if necessary to use public Wi-Fi to protect data and communications from cyberattacks and encrypt all communications.



Caution!

Do not click on any suspicious links received via email, even if the sender appears to be someone you know, as it may be a phishing attempt.

Digital Identity Security and Password Security

To protect digital identity, consider the following:

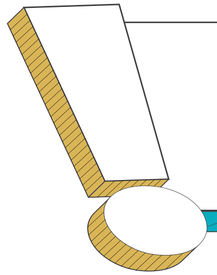
Create strong passwords that are difficult to guess and use a password manager to store them securely to protect them from theft.

Choose passwords composed of a mix of letters, numbers, and symbols.

If you wish to add another security layer, two-factor authentication can achieve this.

Do not use the same password for multiple accounts or services.

Change passwords regularly.



Facts and Information

Phishing is one of the most common attack methods, enticing users to provide their personal information through fake messages.

Digital Identity Protection Measures

Monitoring Bank Accounts

Regularly checking bank accounts online is essential to monitor any suspicious activity and take appropriate action to prevent significant damage to funds or reputation.

Caution When Disposing of Important Data

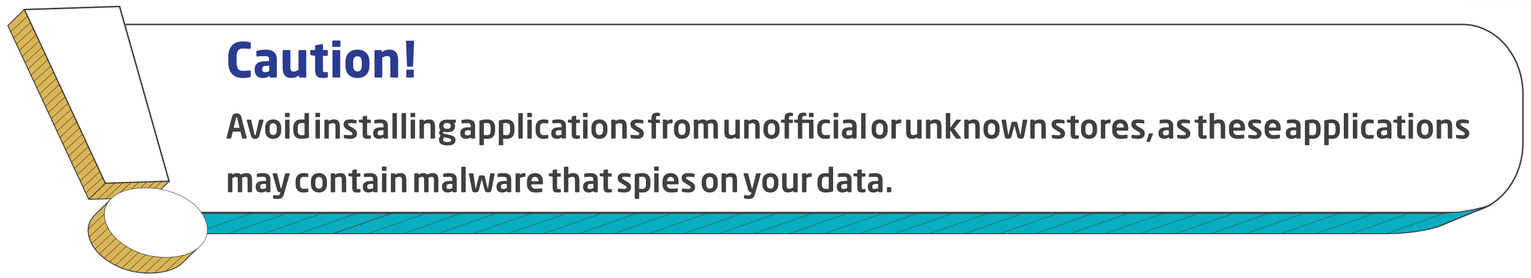
When disposing of papers or documents containing personal or important information, they should be disposed of securely to avoid them falling into the hands of fraudsters.

This also applies to computers and phones; if you wish to sell and replace them with new ones, you must ensure that all personal data stored on them is deleted.

Digital Footprint and Identity Protection

Over-sharing personal data on social media can help criminals steal digital identities.

The **digital footprint** is one of the main reasons for online identity theft crimes; with the details and information users publish about their personal lives, which are stored for years, these details become available to fraudsters to exploit. Therefore, caution should be exercised regarding the type of information published.



Caution!

Avoid installing applications from unofficial or unknown stores, as these applications may contain malware that spies on your data.

Online Identity Theft Protection

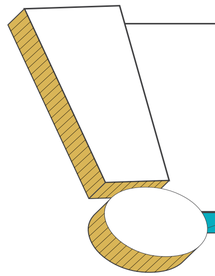
01 Ensure the web address begins with https and not http; the ‘s’ indicates security and look for the lock icon next to the link.

02 Contact the sender if you suspect the identity of the email sender.

03 Enable automatic updates for all programs, applications, and web browsers.

04 Install antivirus and anti-malware software.

05 Do not grant strangers remote access to your computer or phone.



Caution!

Do not ignore software and application updates; updates often contain important security patches to protect against new vulnerabilities.

Identity Theft Red Flags

Monitor unusual activity in bank accounts or credit reports due to the use of stolen identity to spend money or open new accounts.

01

Receive bank notifications indicating that money has been spent or the credit limit has been exceeded without your knowledge.

02

Your credit card is declined when attempting to purchase despite having sufficient funds.

03

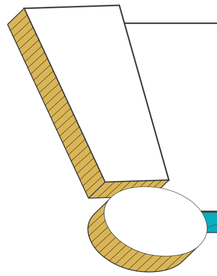
Identity Theft Red Flags

Stop receiving bills via email, which indicates that the criminal has changed the contact details.

04

Inability to log in to bank accounts or social media accounts.

05



Facts and Information

A cyberattack attempt occurs on the internet every 39 seconds, highlighting the continuous threat users face.

Multi-Factor Authentication and Mobile Phone Security

01

Multi-factor authentication is an additional security layer aimed at verifying the user's identity before allowing them to access data.

02

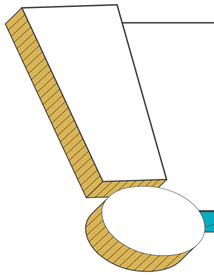
The aim of multi-factor authentication is to prevent unauthorised users from accessing the network or data.

03

It is recommended to adopt strong authentication methods, such as combining passwords, biometric measures such as fingerprint and facial recognition, or personal identification numbers.

04

Multi-factor authentication is one of the effective techniques that provides protection for mobile phones from cyber threats.



Facts and Information

Digital footprint is the trails we leave behind us on the internet, arising from our use of websites, social media platforms, and online purchases.

Updating Mobile Phone Software and Applications

01 Updates are the process of installing new versions of mobile phone programs or systems to enhance their security, fix errors, vulnerabilities, or compatibility issues.

02 It is recommended to update regularly or enable automatic updates.

03 Updated mobile phone applications and systems provide security for the mobile phone and protect it from breaches.

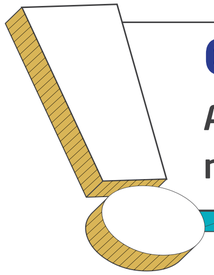
Managing Mobile Phone Permissions

Permissions are the process of controlling access to specific features or functions on phones or applications.

Permissions contribute to enhancing the privacy and security of the device.

Permissions can be used to determine the data that can be accessed, used, or shared.

Caution must be exercised when managing permissions, granting the minimum access necessary to perform tasks only, regularly reviewing and cancelling permissions, and avoiding granting them to unknown sources.



Caution!

Avoid sharing your personal information, such as ID number, address, or phone number, on sites or platforms whose security you are not sure of.

Protection Against Ransomware

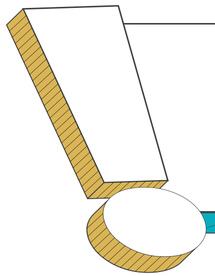
- Install modern and effective antivirus software.
- Update the device’s operating system.
- Scan external storage media before connecting it to the device.
- Use strong passwords and change them periodically.

Protection Against Ransomware

Do not open email attachments from unknown senders.

Avoid opening pop-up ads on websites.

Back up data regularly.



Facts and Information

Companies that rely on the Internet of Things in the industry increase their production efficiency by 25% through improved equipment monitoring.

Best Practices for Risk Mitigation

01 Access Management

Ensure that permissions are granted only to employees who require them to perform their duties.

02 System Updates

Maintain up-to-date operating systems and software to address security vulnerabilities.

03 Continuous Training

Educate employees about cyber threats and how to respond appropriately.

04 Encryption

Utilise encryption to safeguard sensitive data during transmission and storage.

05 Continuous Monitoring

Deploy tools to detect and monitor unusual activities within systems.

Tailored Security Policies and Procedures

Penetration Testing

Conduct regular tests to identify vulnerabilities in systems.

1

2

Incident Response Plan

Develop a clear plan to address cyberattacks and minimise their impact.

Data Backup

Maintain regular backups of data stored securely in safe locations.

3

4

Multi-Factor Authentication (MFA)

Add additional layers of security to login processes.

Partnerships with Cybersecurity Experts

Collaborate with specialised firms to enhance security measures and counter evolving threats.

5

Conclusion

Digital safety is a shared responsibility that demands awareness and vigilance. To safeguard civil society organisations from cyber threats, practical steps must follow, such as adopting strong passwords, enabling two-factor authentication, and regularly updating systems. Moreover, implementing incident response plans and providing employees with training on cyber threats are essential measures.

These practices are not merely precautionary but vital steps to ensure the continuity of services and maintain public trust in the ability of these organisations to protect their data and interests.

Through awareness and commitment to these critical measures, we can all contribute to fostering a secure digital environment and enhancing cybersecurity and digital safety within our communities.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative