General Principles of Digital Safety

Cybersecurity Woman

Target Group
Women

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety
Cybersecurity Woman

Target Group

Women

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

Intellectual Property Rights

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 fundamental to ensuring information security and protecting individuals and communities against ever-increasing cybersecurity threats.

This booklet is intended to raise women's awareness of digital safety principles and best practices to help them avoid risks in cyberspace.

This booklet aims to raise awareness among women and girls about the importance of digital security and its role in protecting their privacy and digital lives. It outlines the key risks they may encounter in cyberspace, including online violence, online harassment, cyberstalking, phishing, digital identity theft, and deepfakes.

The booklet also provides practical guidance and preventive measures to help women secure their personal devices and online accounts, and to respond appropriately to digital threats or abuse. It promotes a culture of safe and responsible technology use.

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.

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

Initiative Overview

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

These activities promote awareness of digital safety, encourage the safe use of the internet and technological applications, explain potential risks, and support the development of a society that is secure in cyberspace and technologically capable.

Target Groups

The Initiative targets various segments of society with a first-year focus on the following groups:

Senior Citizens

Women and Family

People with special needs

University Students

The Financial and Banking Sector

Civil Society Organisations

Expatriate Workers

Awareness-Raising Tools

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

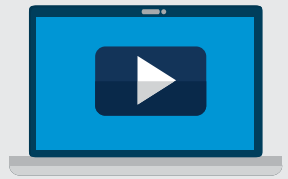
Cybersecurity Games

Awareness-Raising Booklets

Digital Safety Guide

Awareness-Raising Workshops

Innovative Educational Games



Awareness-Raising Videos

01 | Focus area

Digital Safety Essentials

Concept of Digital Safety

Digital security comprises practices and procedures intended to protect personal data and ensure the safe use of modern technologies.

This concept helps to empower women to engage confidently in cyberspace, without fear of exploitation or tracking.

Key Objectives of Digital Safety

1. Protecting data against unauthorised access or use.
2. Empowering users to engage with the internet confidently and responsibly.
3. Preventing cybercrime, including phishing, hacking and cyber harassment.
4. Promoting a culture of cybersecurity awareness across society.
5. Enhancing users' ability to discern reliable from misleading content.
6. Supporting the adoption of preventive measures to minimise digital risks.

Cybersecurity Awareness

Self-awareness is a foundational element of digital protection; it enables users to make informed decisions while navigating the Internet.

Every conscious action contributes to reducing the likelihood of cyber threats.

Thinking carefully before posting or sharing any content

Avoiding entry of personal data on untrusted websites

Steering clear of unknown or suspicious links and attachments

Reading security warnings instead of skipping them

Avoiding the use of public Wi-Fi for financial activities

Downloading software and applications only from official sources

Staying updated on the latest security developments to understand new threats

Protection of Digital Privacy

Digital privacy is a vital safeguard in an interconnected world characterised by the rapid flow of data.

It involves exercising control over personal data and determining who is authorised to access or process it.

For women, digital privacy is essential to psychological safety and social wellbeing.

Privacy Protection Measures

- Privacy settings for all applications should be reviewed regularly.
- Location data should not be shared while travelling or while on the move.
- Outdated or unnecessary photos and posts should be deleted.
- Only friend requests from known and trusted accounts should be accepted.
- Access to posts and comments on social media accounts should be limited.
- Account names should not include directly identifying personal data.
- Frequent sharing of everyday personal details should be avoided.
- Registration on websites that request more personal data than is necessary should be avoided.

Device Security

Smart devices are the primary means of access to cyberspace; therefore, their protection is critical.

Essential Steps to Secure Devices

- A device lock using a strong PIN or alphanumeric passcode should be enabled, with biometric authentication activated where available.
- The operating system and applications should be kept up to date to patch security vulnerabilities.
- The 'Find My Device' feature should be enabled to locate a device if lost.
- Applications that are untrusted or that request excessive permissions should be uninstalled.
- Automatic connection to public Wi-Fi networks should be disabled
- Antivirus software should be installed and kept up to date
- Sensitive files should be stored in encrypted form
- Firewall protection should be enabled to minimise the risk of unauthorised access

Password Management

A password acts as the first line of defence against unauthorised access. The strength of digital protection depends on the robustness and proper management of passwords.

Ways to create and manage passwords

1. Using long passwords containing symbols, numbers, and varied characters
2. Using a unique password for each account or digital service
3. Avoiding personal information or commonly used words
4. Changing passwords regularly—especially after any suspicious activity
5. Using trusted password manager applications
6. Avoiding saving passwords on public devices or browsers
7. Logging out of accounts after completing use

Data and Content Protection

Personal data constitutes a valuable digital asset that should be handled with care; negligent storage or disclosure increases the risk of exploitation and unauthorised access.

Guidelines for Data Security

1. End-to-end encrypted messaging applications should be used
2. Sensitive images or documents should not be sent by email or shared in public chats
3. Important files should be backed up regularly, and the backups should be encrypted
4. Messages that are old or that contain personal data should be deleted
5. Private files should be stored on offline storage media
6. Images and documents should be protected using reputable, up-to-date encryption software
7. All data should be securely and irreversibly wiped before any device is sold or reformatted

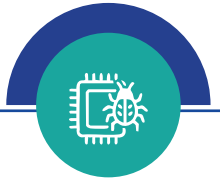
Handling Digital Threats

A calm, methodical approach to digital risk reduces its potential impact, as the correct response is the first step towards a solution.

Procedures for Responding to a Digital Threat

Abusive messages or content should be documented using screenshots

Hostile messages or messages from unknown sources should not be answered



Suspicious accounts should be blocked immediately

Passwords should be changed, and affected accounts secured

Contacting technical support or relevant authorities

Digital evidence should be preserved in anticipation of any legal action

Sustainable Digital Security Practices

Digital safety is not a one-time task but an ongoing effort.

Consistent implementation of preventive measures strengthens long-term digital protection.

Ongoing Preventive Practices

- Updating systems and applications as soon as updates are available
- Conducting monthly reviews of security settings
- Enabling two-factor authentication on all sensitive accounts
- Monitoring accounts and devices for unusual activities
- Spreading awareness on digital safety among friends and colleagues
- Adopting a “think before you click” mentality in all online interactions

02 | Focus area

Safe Behaviour in Cyberspace

Digital Threats Faced by Women and Girls

Digital violence

Online Harassment

Cyberstalking

Threats and blackmail through the internet

Personal Data Theft

Safe Digital Behaviour

Safe behaviour in cyberspace refers to a set of conscious practices aimed at using technology and the Internet responsibly, reducing risks, and protecting the digital privacy and safety of women and girls.

It includes mindful interaction with information and published content on online platforms

Based on awareness of one's rights and responsibilities within cyberspace

Serves as a foundation for building a safe digital environment characterised by trust and mutual respect

Helps reduce cybercrimes that stem from irresponsible online behaviour

Managing Personal Information

Personal information is among the most valuable assets in digital environments, and protecting it requires continuous effort.

1. Avoiding the disclosure of sensitive data in chats or public comments
2. Using official email accounts only for professional communications
3. Reviewing privacy policies before submitting any online information
4. Storing important data in secure and encrypted locations
5. Regularly deleting outdated or unnecessary information

Safe Use of Devices and Applications

Smart and conscious device usage reduces the likelihood of hacking or data loss.

- Installing only trusted apps from official stores
- Activating auto-lock features and using strong passwords
- Avoiding device or account sharing unless absolutely necessary
- Avoiding connection to untrusted public Wi-Fi networks
- Monitoring app permissions and ensuring they align with the app's purpose

Cyber Violence

Online violence refers to any hostile or threatening behaviour perpetrated via the internet or digital platforms and directed at women.

It seeks to cause psychological, social, or even financial harm by weaponising technology.

1. Includes threats, blackmail, defamation, and the sharing of offensive content
2. May be direct or indirect through messages or comments
3. Often causes deep psychological effects such as anxiety, depression, and reduced self-esteem
4. Increases feelings of isolation and detachment from the digital community
5. Requires community awareness to recognise and reduce its spread

Online Harassment

Digital harassment is one of the most widespread forms of online violence, primarily targeting women and girls.

01 It appears through unwanted messages, offensive photos, or videos and offensive comments

02 Perpetrators may use fake accounts to hide their identities

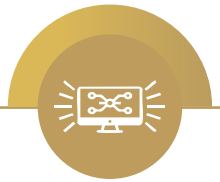
03 Can occur via email, social media, or messaging applications

04 Reduces digital freedom and confidence when navigating online spaces

05 Ignoring harmful messages or blocking the sender is a primary step to minimise harm

Cyberstalking

Cyberstalking involves persistently following or monitoring someone online without their consent. It can begin subtly and escalate into a continuous threat.

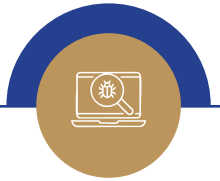


Includes monitoring posts, comments, and the user's online presence

May start with gathering personal information and escalate into direct threats

It causes a persistent sense of fear and loss of digital safety

Threatens personal and social privacy and restricts digital freedom



Keeping digital evidence and reporting to relevant authorities helps reduce harm

Preventing Violence and Harassment

Awareness-based approaches to dealing with online violence and harassment help reduce risks and limit their spread.

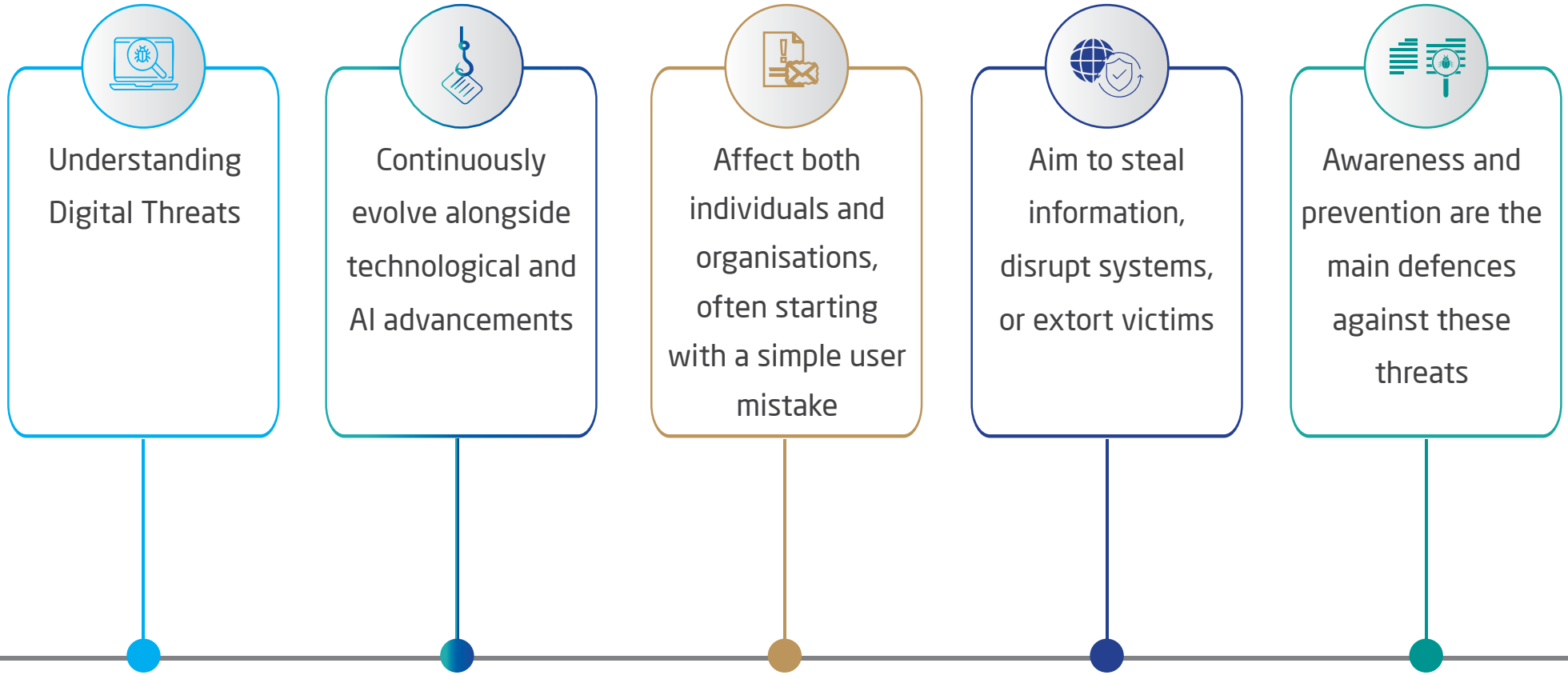
1. Using blocking and reporting tools available on digital platforms
2. Protecting personal information and avoiding the sharing of live location or sensitive data
3. Regularly reviewing privacy settings to minimise exposure
4. Keep digital evidence: such as messages or screenshots; for legal documentation
5. Seeking assistance from relevant authorities or psychological support if matters escalate
6. Promoting awareness about online violence and methods of prevention within the community

03 | Focus area

Digital Threats and Preventive Measures

Understanding Digital Threats

Digital threats refer to a range of risks targeting devices, data, or digital identities, varying in method and severity.



Phishing and Cyber Fraud

Phishing is one of the most widespread cyber-attacks, relying on deception to trick users into voluntarily giving away their information.

01 Often appears through emails, text messages, or fake advertisements

02 Attackers use urgent phrases such as “update your account” or “your bank card will be suspended”

03 Messages include fake links leading to counterfeit websites mimicking legitimate ones

04 Once the victim interacts, attackers collect passwords or financial details

05 Ignore suspicious messages and verify the sender through official channels

06 Enable two-factor authentication to reduce the success rate of phishing attempts

Malware

Malware refers to harmful software intentionally placed on devices to damage, steal, or exploit data. Ransomware is considered one of the most dangerous forms of malware.

it spreads through attachments, pirated apps, or unsafe websites

01

Ransomware encrypts files and demands money to restore access

02

Infected devices often slow down or behave unusually

03

Even after paying the ransom, there is no guarantee that the data will be restored

04

Protection requires encrypted backups and continuously updated security software

05

Avoid installing any files or applications from unknown sources

06

Identity Theft

Identity theft occurs when someone uses another person's information without their consent

1. The targeted data includes photos, card numbers, or social media accounts
2. Stolen data may be used for financial fraud, blackmail, or defamation
3. Reducing the sharing of sensitive data and managing passwords responsibly helps prevent impersonation
4. Regularly monitoring account activities helps detect threats early
5. Oversharing personal content online makes impersonation easier
6. Some cases can be detected through login alerts or unusual verification attempts

Deepfakes

Deepfake refers to AI-generated images or videos that appear realistic and are difficult to distinguish from real content.

1. May be used to damage reputations or extort individuals
2. Spread quickly online due to their shocking nature
3. Can influence public opinion or create social and political crises
4. Prevention requires verifying the source before reposting or sharing
5. Using deception-detection tools and image-analysis technologies enhances awareness of digital content
6. Digital media literacy is one of the most effective ways to reduce the spread of misinformation

Social Engineering

Social engineering relies on exploiting human trust or curiosity to obtain information without the need for technical hacking.

Attackers pose as official employees or trusted organisations to request sensitive information

They may send friendly messages or tempting offers to build trust

They use emotions such as fear, sympathy, or urgency to encourage victims to reveal information

Often begins with a simple question, then escalates to requesting sensitive data

Awareness of these deception techniques serves as the first line of defence

It is advised not to share any information unless the identity of the requesting party has been verified

Malicious Apps and Links

Untrusted applications and harmful links are among the most common tools used to hack devices and steal data.

Some apps request excessive permissions unrelated to their function

Downloading apps from unknown sources often leads to malware installation

Shortened or unfamiliar links are commonly used in scams

It is preferable to download applications only from approved official stores

Regularly reviewing app permissions is an essential security step

Ignore any link sent from an unknown source, even if it appears familiar on the surface

Cloud Storage

Cloud storage is convenient but requires careful management to prevent data leaks or unauthorised access.

01 Uploading sensitive files without encryption exposes them to misuse

02 Free cloud services may not offer strong security

03 Public sharing links can grant full access to files

04 Use reputable cloud services and enable two-factor authentication (2FA)

05 Deleting old files and reducing the sharing of open links enhances protection

06 Encrypted backups of sensitive data help maintain continuous security

Regular Updates

Security updates and digital education are essential components of cybersecurity.

1. Companies release updates to fix discovered vulnerabilities
2. Delaying updates leaves devices open to attacks
3. Enabling automatic updates ensures immediate protection
4. Restarting devices after updates is necessary to activate fixes
5. Continuous learning about phishing and cyber scams increases personal safety
6. Participating in cybersecurity awareness workshops supports a safer digital community

References

1. ernest, nonum et al. SOCIAL ENGINEERING: UNDERSTANDING HUMAN FACTORS IN CYBER SECURITY. International Journal of Convergent and Informatics Science Research. May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326
2. eSafety Commissioner (Australia). Staying safe: Cyberstalking, on site: https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking
3. European Institute for Gender Equality. Cyber violence against women, on site: https://www.eige.europa.eu/gender-based-violence/cyber-violence-against-women
4. European Parliament. (2023). IPOL_STU(2023)743341_EN [PDF]. on site: https://www.europarl.europa.eu/RegData/etudes/STUD/2023743341//IPOL_STU(2023)743341_EN.pdf
5. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware
6. Karnouskos, Stamatis. Artificial Intelligence in Digital Media: The Era of Deepfakes, IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, June 2020, on site: https://ieeexplore.ieee.org/document/9123958
7. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing
8. Kosinski, Matthew. IBM. What is ransomware? Retrieved, on site: https://www.ibm.com/think/topics/ransomware

9. National Cyber Security Centre. Password policy: updating your approach. November 2018, on site: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

10. Startup Defense. Fake software update prompts. on site: https://www.startupdefense.io/cyberattacks/fake-software-update-prompts

11. UN Women. FAQs: Digital abuse, trolling, stalking and other forms of technology-facilitated violence against women. February 2025, on site: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

12. United Nations Office on Drugs and Crime. Handling of digital evidence (Module 6), on site: https://www.unodc.org/e4j/ar/cybercrime/module-6/key-issues/handling-of-digital-evidence.html