الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Audience
University Students

Teacher'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

General Principles of Digital Safety

Target Group

University Students

Teacher's Guide

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

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 Senior Citizens 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.

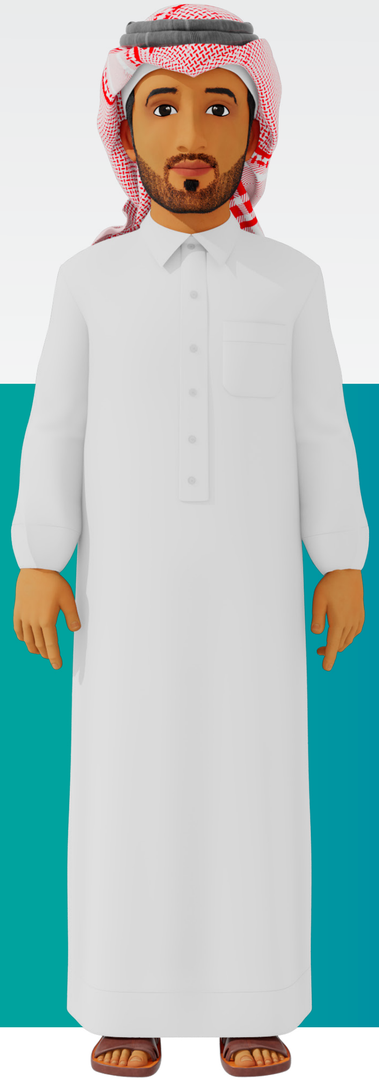
These efforts are part of the National Initiative for Digital Safety, organised by The National Cyber Security Agency, to establish a secure digital environment for all members of society.

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

Online Data Protection

Personal Data

Data

It refers to any information or facts that can be collected and analysed. This includes numbers, text, images, and more. Data plays a crucial role in decision-making and technological advancements.

Personal Data

This is any information that relates to an identifiable individual. It encompasses details such as name, address, phone number, email, financial information, and even electronic addresses.

Examples of personal data include:

National ID number.

Medical and health information.

Bank account details.

Online activities.

Digital Identity Theft

Digital identity theft occurs when an unauthorised individual gains access to another person's identity information online and uses it unlawfully for personal or financial gain. This information includes personal account details, passwords, or financial data.

Examples of stolen data

- National or social numbers
- Bank information
- Credit cards numbers
- Passwords

Caution!

Avoid using unsecured public networks when accessing sensitive data, as they may be vulnerable to attacks that allow attackers to eavesdrop on the connection.

How Does Digital Identity Theft Occur?

1

Phishing

Victims are deceived into revealing sensitive information through fake messages or websites that appear legitimate.

2

Malware

Malicious software is installed on users' devices to collect personal data without their knowledge.

3

Database Breaches

Attackers target companies or institutions to steal large amounts of user data stored on their servers.

4

Brute Force Attacks

Hackers attempt to breach accounts by trying millions of possible password combinations.

Common Methods of Identity Theft

Wi-Fi Eavesdropping

Public Wi-Fi networks are insecure and provide a suitable environment for cybercriminals to intercept personal data of connected users.

Phishing Attacks

Cybercriminals deceive victims into revealing sensitive information such as login credentials or credit card numbers by sending emails that mimic those from known sources like banks.

Malware Attacks such as Ransomware

Malicious software can be used to infiltrate computers and networks, aiming to access or hold personal data hostage until a ransom is paid.

Social Engineering

Social engineering is not a cyberattack, but a set of techniques and tools used by attackers to manipulate victims.

1 | In social engineering, attackers exploit human emotions such as fear, desire, need, and sympathy.

2 | By exploiting these emotions, attackers trick victims into providing sensitive information, which is then used for fraudulent purposes.

Caution!

Avoid sharing your Wi-Fi password with strangers or untrusted individuals, as they may use this connection to access your data.

Information and Data Targeted by Social Engineering Attacks

Attackers aim to obtain the following information through social engineering attacks:

1. Social Security Numbers.
2. Phone Numbers.
3. Banking Records.
4. Personal Data.
5. Important Work Data.

Caution!

Beware of social media apps that request unnecessary permissions to access your personal files or contacts.

Phishing and Exploiting the Desire to Help

Phishing is a type of cyberattack where attackers use fake emails or websites to trick people into revealing sensitive information, such as passwords or banking details.

Phishing and Exploiting the Desire to Help

Attackers exploit the human desire to help others.

They may pose as a charitable organisation, requesting donations to aid the poor or refugees.

Do not trust any entity claiming to be a charity.

Only donate to humanitarian causes through the official websites of well-known charitable institutions.

Request a paper or electronic receipt to verify your financial donation.

Facts and Information

Malware can spread through malicious emails or unreliable downloads from the internet, so caution is advised.

How to Avoid Phishing Attacks

1. Raise awareness on cybersecurity.
2. Think twice before clicking on links in emails or unsolicited messages.
3. Ensure website security by checking that the URL starts with “https” and a closed lock icon appears next to the address bar. Examine the site’s security certificate.
4. Regularly review your online accounts and change your passwords frequently.
5. Monitor your financial data regularly and scrutinise monthly account statements.
6. Update your browser regularly to benefit from security patches available for well-known browsers.

The Safe Use of Shared University Networks

Wireless Networks

Wireless networks are a type of network that uses radio signals or light waves to exchange information between devices without the need for cables. These networks provide flexible and fast connectivity.

Types of Wireless Networks

Wi-Fi

Used in homes and offices to provide internet access to various devices.

Bluetooth

Connects nearby devices, such as phones and headphones.

Cellular Networks

Such as 4G & 5G, which are used to provide mobile phone and data services.

Securing Wireless Networks

- Use Strong Encryption: Implement WPA2-Personal or WPA2-Enterprise encryption for network access.
- Update Software and Firmware: Ensure that network devices and software are up to date.
- Enhance Security Settings: Disable SSID broadcasting to make the network invisible.
- Implement Strong Authentication: Enable two-factor authentication when available.
- Enable Threat Detection and Mitigation: Utilise IDS (Intrusion Detection Systems) or IPS (Intrusion Prevention Systems) for wireless networks.

Safe Use of the Internet

Academic Data Management

Retaining backup copies of projects and academic files on reliable cloud storage services such as Google Drive or OneDrive.

Protecting sensitive files using encryption to ensure unauthorised individuals cannot access them.

Deleting academic files from public or shared devices immediately after use.

Email Security

Email

It is a well-known means of communication for individuals and businesses, containing sensitive information and data.

Maintaining email security is crucial to protect sensitive information and prevent fraud and cyberattacks.

Common Threats

Spam, phishing, malware, and malicious links.

Spam Emails

- Spam: Unwanted messages sent in large quantities.
- Often contains unsolicited commercial offers and advertisements.
- The best way to protect against spam is to use email filters.

Facts and Information

Using encryption techniques is one of the best ways to protect data during online transmission.

Email Protection Measures

Monitoring unusual activities on your email account can help detect attacks in their early stages.

Regularly backing up your emails ensures you don’t lose important data in case of an attack or system malfunction.

Updating email software and operating systems regularly reduces the risk of exploiting security vulnerabilities.

Passwords

A password is a sequence of characters, numbers, and symbols used to verify a user's identity and grant them access to specific accounts or data.

Importance of Passwords

1

Protecting Information

Passwords prevent unauthorised access to sensitive information, such as bank accounts, email, and personal data.

Digital Security

Passwords are the first line of defence against breaches and cyberattacks.

2

Best Practices for Password Protection

- Use Password Management Software.
- Be Wary of Phishing Emails.
- Enable Two-Factor Authentication (2FA).
- Do not write down passwords on paper or in files but store them in a password management program.
- Change Passwords Regularly.
- Log out when using shared computers.

Facts and Information

Cyberattacks on social networks aim to steal personal data and use it for online fraud.

Attacks Targeting Passwords

1. Brute Force Attacks.
2. Dictionary Attacks.
3. Phishing Attacks.
4. Password Spraying Attacks.
5. Keylogging Attacks.

Passwords Manager

A password manager is a tool that helps users create, store, and manage passwords securely.

Password managers are available as applications or browser extensions.

They offer numerous features to enhance personal security and protect sensitive information.

Facts and Information

Improving cybersecurity starts with understanding system vulnerabilities and proactively addressing these loopholes.

Advantages of Using a Password Manager

1

Encrypted Storage

Password managers encrypt all login credentials and passwords using strong encryption techniques.

2

Local Decryption

Decryption is performed only on the local device using a master password.

3

Generating Strong Passwords

Password managers can generate strong and unique passwords for each account, enhancing account security.

4

Synchronisation

Automatic synchronisation between devices allows users to access passwords from anywhere.

5

Protection Against Phishing

Password managers reduce the risk of phishing attacks by only filling in information on trusted sites.

6

Password Strength Checks

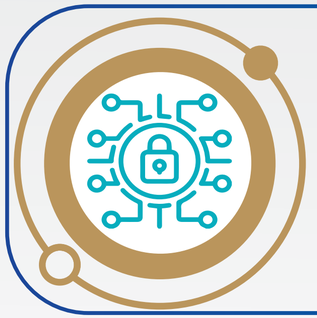
Password managers report the strength of used passwords and advise updating them if they are weak.

7

Breach Alerts

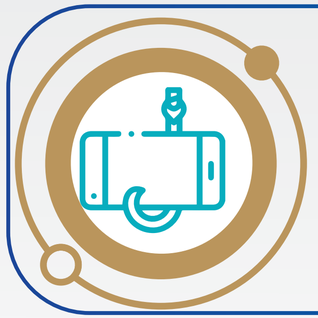
Password managers notify users if a security breach related to one of their accounts is detected.

Benefits of Two-Factor Authentication (2FA)



Increased Security

It adds an extra layer of protection beyond the password, making it difficult for attackers to access accounts even if they obtain the password.



Protection Against Phishing Attacks

Even if a user is tricked into providing their password through a phishing attack, the attacker cannot access the account without the second verification code.

Protection Against Brute Force Attacks

Two-factor authentication makes brute force attacks less effective because attackers must overcome the second verification layer.

Alerts for Unusual Activity

In many systems, if two-factor authentication is enabled, users receive alerts about unusual login attempts, allowing them to take immediate action.

Facts and Information

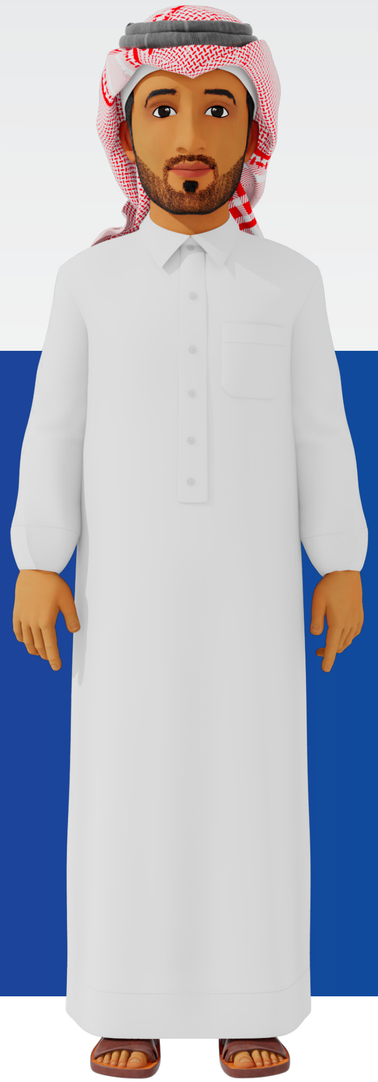
Quantum computing poses a new challenge to cybersecurity, as it can impact current encryption techniques.

Conclusion

Digital safety is a shared responsibility that requires awareness and vigilance. By following simple tips such as using strong passwords, enabling two-factor authentication, avoiding suspicious links, steering clear of unsecured public networks, regularly updating devices and software, and attending cybersecurity awareness courses within the university. Thus, we can enhance our protection against cyber threats.

By adhering to the implementation of these significant measures, students can focus on their studies with confidence, while ensuring the security of their digital data.

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



Before closing, please take a moment to fill out your personal information and evaluate the workshop. Scan the below QR:

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency