الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Audience

Expatriate Workers

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 in Digital Safety

Target Group

Expatriate Workers

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.

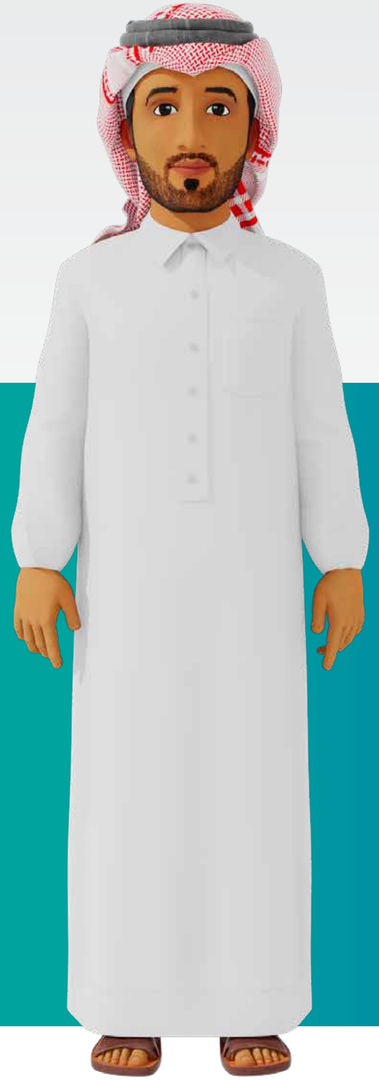
This booklet has been developed to raise awareness among people with special needs about the principles of digital safety and the best practices that help them avoid cyber threats. It aims to enhance their understanding of key risks, such as phishing, identity theft, and malware, emphasising the importance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

Scope of the Initiative

A set of awareness activities in digital safety and cybersecurity, targeting the local community across all age groups, social backgrounds, and professional sectors. The initiative aims to raise awareness of digital safety and the secure use of the Internet and various technological tools while clarifying potential risks, with the goal of building a society that is secure in cyberspace and capable in the use of technology.

Targeted Groups



The initiative addresses all societal groups. During its first year, primary focus will be directed towards the following groups:

- Senior Citizens
- Women and Family
- People with special needs
- University Students
- Expatriate Workers
- Civil Society Organisations
- The Financial and Banking Sector

Awareness-raising tools

The initiative employs a set of varied and integrated awareness tools, which include the following:

- Digital Safety Guide
- Awareness-Raising Booklets
- Cybersecurity games

- Awareness-Raising Videos
- Innovative Educational Games
- Awareness-Raising Workshops

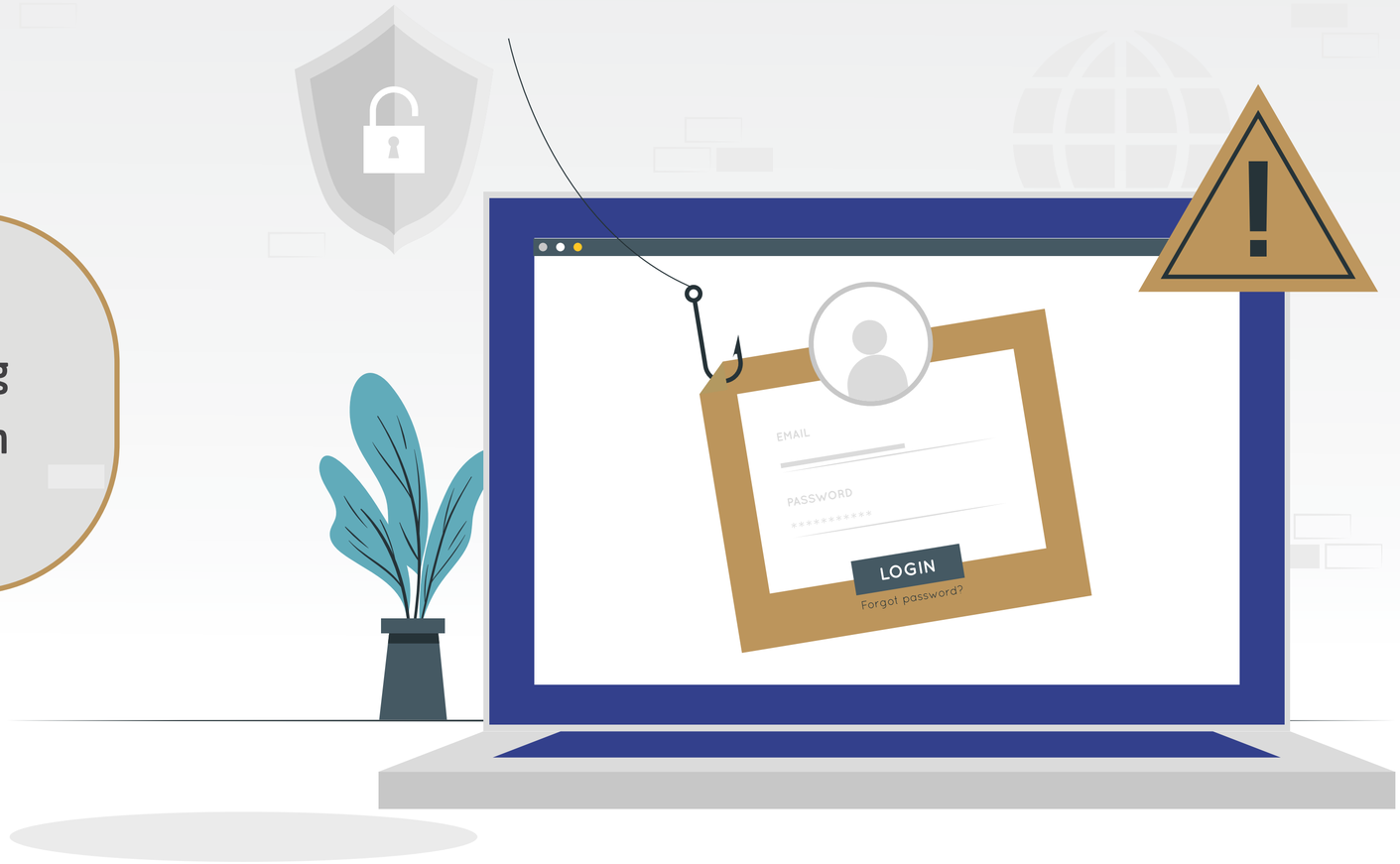
Common Cyber Risks

Phishing

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

Facts and Information

Ransomware attacks operate by encrypting victims' files and demanding payment in exchange for decrypting them.



How Phishing Attacks Are Executed

Fraudulent Messages

The attacker sends an email that appears to be from a trusted source, such as a bank or well-known company.

Fake Websites

The message contains a link directing to a fake website resembling the original site, where the victim is prompted to enter their personal information.

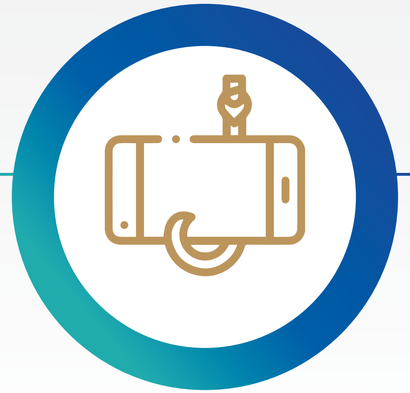
Information Exploitation

Once the victim provides their data, it is used to steal money or access their private accounts.

Methods of Executing Phishing Attacks

Emails and fraudulent messages that appear legitimate.

Pop-up windows and misleading advertisements.



Fraudulent phone calls or voicemail messages.

Fake promotional offers.

Risks of Phishing

1

Theft of Personal Data

Obtaining sensitive information such as passwords and bank card details.

2

Financial Account Compromise

Gaining access to bank accounts and stealing funds.

3

Cyber Extortion

Using stolen data to pressure victims into paying a ransom.

4

Device Infection with Malicious Software

Injecting harmful software when victims click on fraudulent links.

5

Identity Theft

Exploiting stolen information to engage in illegal activities under the victim's identity.

Personal Data Theft

Personal data theft is among the most critical cybercrimes targeting individuals and organisations. It involves the unauthorised acquisition of sensitive information, such as identification numbers, passwords, or bank account details, for illegal activities.

With the increasing reliance on technology, protecting personal data has become a necessity to mitigate the risks associated with these crimes.

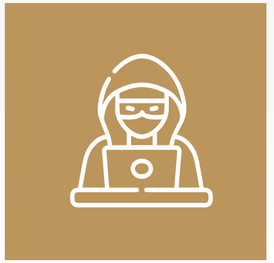
Malware

Malware is malicious software designed to harm computers or networks or steal data without user knowledge. Types of malwares include viruses, worms, spyware and others.

How Does Malware Work?

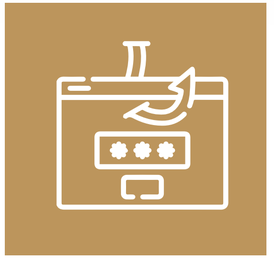
1 | **System Infection**

Malware is planted in the system through downloading suspicious files or clicking unsafe links.



2 | **Stealthy Execution**

Once installed, the malware operates silently without the user noticing immediate changes.



3 | **Data Theft or System Disruption**

Malware can steal user data, disable systems or cause financial losses.

Signs of Malware Infection

1

Device Performance Decline

Malware consumes system resources.

2

Unwanted Pop-up Windows

This includes repeated ads and fake threat warnings.

3

Sudden System Changes

This involves browser homepage changes and new toolbars appearing.

4

Unexplained high data consumption.

5

Automatic email sending.

6

New files/ folders appearing or disappearing.

Spyware

Spyware is a type of malicious software that collects information about users without their knowledge or consent, including the following types:

- **Keyloggers:** Software allowing attackers to steal passwords, personal and financial data entered via keyboard.
- **Adware:** Software that displays unwanted advertisements on the user's device and collects data about user browsing.
- **Tracking Cookies:** Small text files stored on the user's device to track their internet activity.
- **System Monitors:** Software that monitors system activity and collects data about computer usage.

Warning!

Avoid sending sensitive data, such as passwords or banking information, through unencrypted communications. Always use secure channels.

Spyware on Camera

1. Software that automatically activates the smartphone or computer camera.

2. The software transmits recorded video to the attacker, with the intent of invading the victim's privacy or extorting them financially.

Facts and Information

Small and medium-sized businesses are generally less equipped to manage cyberattacks, making them frequent targets for hackers.

Risks of Spyware

1

Identity Theft

Spyware targets victims' digital identity and personal data.

2

Blackmail

Using stolen sensitive information to blackmail victims.

3

Loss of Privacy

Tracking internet activity and collecting personal data without user knowledge violates privacy.

4

Device Performance Decline

Spyware slows down devices due to data collection processes.

Facts and Information

Smart home devices that rely on the Internet of Things can be vulnerable to hacking if not secured properly.

Preventative Measures and Tips

How to Identify Fraudulent Emails and Messages

1. The sender's email or phone number does not match the known name of the institution.
2. The email or phone number used differs from the official contact information published by the institution being impersonated.
3. The URL in the message may appear legitimate but does not match the official website of the institution.
4. The message noticeably differs from previous communications received from the institution.
5. The message requests sensitive personal information, such as a credit card number or account password.
6. The messages are unsolicited and contain unexpected attachments.

Warning!

Emails requesting personal or financial information may be part of phishing attempts aimed at stealing your identity.

Protection from Phishing

- Never provide information to anyone before fully verifying their identity.
- Banks and financial institutions never request confidential data from customers by phone.
- Install and regularly update antivirus software.
- Create backups of data on external hard drives or in the cloud.

Ways to Avoid Phishing Attacks

1. Raise cyber awareness.
2. Carefully consider before clicking on links in random emails and instant messages.
3. Confirm the website's security by checking that its address begins with https and that a closed padlock icon is next to the address bar.
4. Regularly check online accounts and change passwords periodically.
5. Regular monitoring of financial data and careful review of monthly account statements.
6. Update browsers regularly to benefit from security patches for common browsers.

Warning!

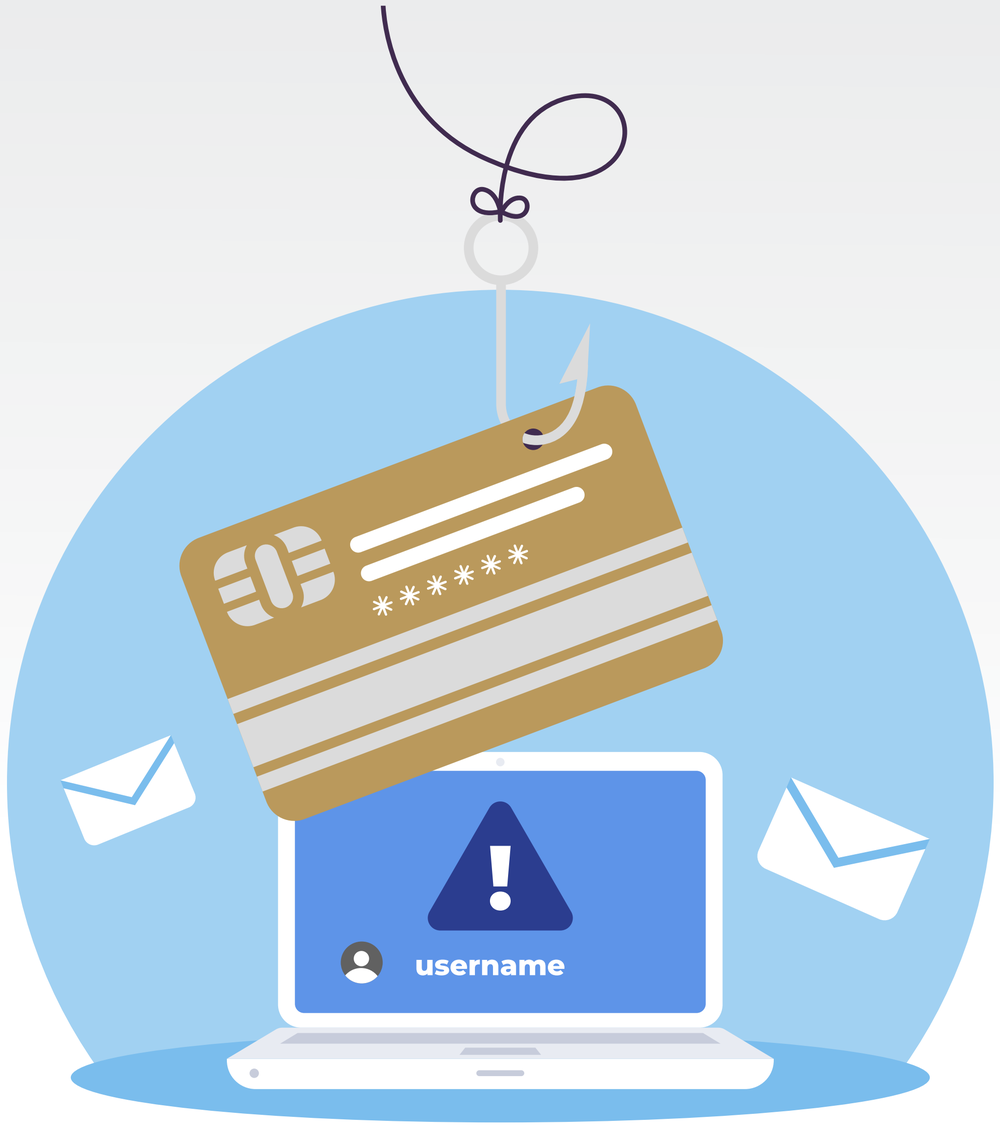
Beware of installing software from untrusted sites; unlicensed programmes may be infected with malware.

Practical Tips for Preventing Phishing

- Ignore suspicious messages requesting sensitive information.
- Always verify the identity of the sender before engaging with the message.
- Use antivirus software and email services with built-in phishing filters.
- Inspect website URLs carefully and avoid accessing them if they seem unreliable.

Facts and Information

Weak passwords significantly simplify the process for attackers to gain unauthorised access to accounts, emphasising the importance of using strong, secure passwords.



Responding to Malware Infections

1. Disconnect your device from the internet.
2. Use Safe Mode.
3. Use malware removal tools.
4. Update operating system and programmes.
5. Restore system.
6. Review account security.

Warning!

Do not use the same password for all your online accounts. If one account is compromised, all accounts will be at risk.

Prevention Measures Against Identity Theft

Use Strong Passwords

Complex and unpredictable passwords.

Enable Two-Factor Authentication

Add an extra layer of protection.

Avoid Suspicious Links and Files

Don’t click on suspicious links or download untrusted files.

Facts and Information

Two-factor authentication is one of the most effective methods for protecting personal accounts from cyber breaches.

Steps to Follow in the Event of Data Theft

Report to Authorities

Inform agencies responsible for combating cybercrimes.

Change Passwords Immediately

Change all passwords for affected accounts.

Monitor Financial Accounts

Monitor bank accounts and credit cards to detect any suspicious activity.

Protection from Spyware on Camera

Avoid downloading or opening unknown links.

If the camera activates automatically, stop using the smartphone and seek expert consultation.

Regularly scan devices for malware.

Manually verify the camera is turned off.

Cybersecurity Assurance

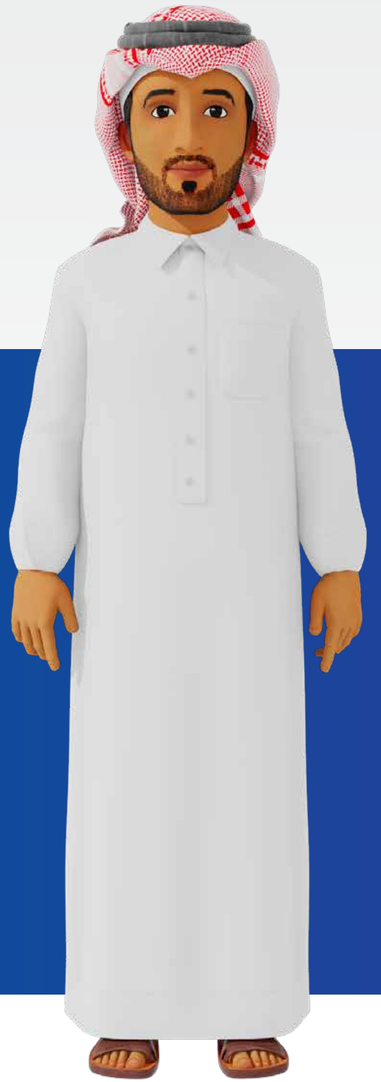
What to Do	What to Avoid
Use strong and complex passwords.	Using simple, easily guessed passwords.
Enable two-factor authentication for accounts.	Ignoring additional security settings when logging in.
Regularly update operating systems and software.	Postponing or neglecting essential updates.
Verify the legitimacy of links before clicking.	Clicking on links from unknown sources.
Periodically review bank and financial accounts.	Neglecting to check financial statements.
Download applications only from trusted sources.	Installing software or apps from unverified websites.
Be cautious of messages requesting personal information.	Sharing personal information via email or messages.
Install antivirus software and regularly scan devices.	Operating without effective cybersecurity measures.

Conclusion

Digital safety is a shared responsibility that demands awareness and vigilance. By adopting straightforward practices, such as using strong passwords, enabling two-factor authentication, avoiding suspicious links, and consistently updating devices and apps, we can bolster our protection against cyber threats. Remember the importance of regularly reviewing financial accounts and avoiding sharing personal information through insecure channels.

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.

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



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative