الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Audience

Financial and Banking Sector

Teacher's Guide

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Audience

Financial and Banking Sector

Teacher's Guide

Intellectual Property Rights

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Contact the National Cyber Excellence Department

00974 404 663 79
00974 404 663 62
www.ncsa.gov.qa/
academy@ncsa.gov.qa

Table of content	Page

Table of content	Page

Introduction

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

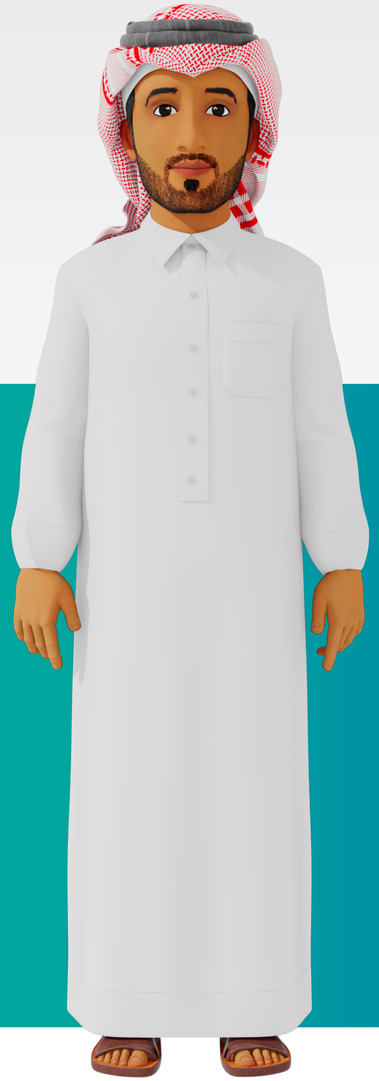
This booklet has been developed to raise awareness among the financial and banking Sector about the principles of digital safety and the best practices that help them avoid cyber threats. It aims to enhance their understanding of key risks, such as phishing, identity theft, and malware, enabling them to effectively protect their data and devices.

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

Cybers Risks in the Financial and Banking Sector

Financial Transactions through Unknown Parties

Money transfer is the process of exchanging funds between individuals or entities through various channels, including banks, electronic financial services, and mobile transfers.

Security of Financial Transactions

01 Refrain from conducting money transactions with unverified entities

02 Verify recipient identity prior to transfers

03 Utilize trusted methods for counterparty verification

04 Avoid dealings with unknown individuals or companies

05 Exercise caution regarding suspicious online financial offers

Facts and Information

Regular training on cybersecurity best practices for corporate personnel can significantly minimize the likelihood of security breaches.

Phishing

Phishing is among the most severe cybersecurity threats facing the financial and banking sector. Attackers use fraudulent emails or fake websites to deceive employees and clients into disclosing sensitive information, such as passwords or bank account details.

Risks of Phishing

1. **Theft of Banking Data: Acquiring sensitive information such as login credentials or bank card details, thereby jeopardising the financial accounts of institutions and individuals.**

2. **Financial Account Breach: Exploiting stolen data to gain access to bank accounts and steal or transfer funds.**

3. **Financial Extortion: Leveraging stolen information to blackmail institutions or individuals for monetary gain.**

4. **Malware infection: Infecting financial systems with malicious software through interaction with fake links, leading to operational disruptions or data theft.**

5. **Identity Theft: Using stolen information to conduct financial transactions or fraudulent activities in the victim's name, damaging the institution's reputation.**

Remote Meetings

- **Unauthorised Access:** Attackers may breach meetings and leak critical information.
- **Phishing Attacks:** Fake meeting invitations may target users to steal login credentials or other sensitive information.
- **Espionage:** Attackers may eavesdrop on sensitive discussions and expose confidential data.

Device Security

Device security in the financial and banking sector is a critical priority to ensure the protection of sensitive data and financial transactions. This includes:

01 Securing computers, mobile phones, and tablets used in financial institutions with antivirus software.

02 Updating system regularly to patch security vulnerabilities and enabling encryption to protect stored and transmitted data.

03 Implementing strict access control policies including using a strong password and activating two-factor authentication.

Common Cyber Threats

Ransomware

Ransomware is malicious software that encrypts user data or locks devices, preventing access to files or systems. Attackers typically demand a monetary ransom in exchange for decryption keys or system access restoration.

Ransomware Attack Methodology

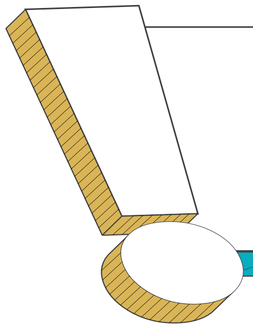
1. **System Infiltration:** Typically occurs through email attachments, suspicious websites, pop-up advertisements, or system vulnerabilities

2. **File Encryption:** Upon infiltration, the malware encrypts crucial files, including documents, images, and databases

3. **Ransom Demand:** Post-encryption, victims receive a message demanding payment for decryption keys

Risks of Ransomware

1. **Data Encryption:** Ransomware encrypts files, making data inaccessible unless the ransom is paid.
2. **Data Theft:** Attackers not only encrypt data but steal them as well.
3. **Business Disruption:** Cyber-attacks can result in complete operational disruption.
4. **Anxiety and Stress:** Such attacks can cause significant stress, particularly when sensitive data is compromised.
5. **Recovery Delay:** System and data restoration can be significantly time-consuming.



Warning!

Avoid public Wi-Fi networks when conducting banking transactions or login to sensitive accounts as this is a common target for hackers

Whaling - Targeted Phishing Attacks

A type of phishing attack targeting high-profile individuals within organisations, such as executive directors, board members, and senior staff.

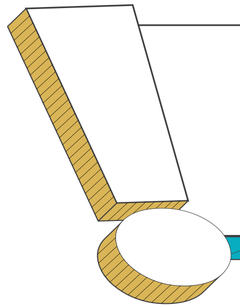
The attack aims to obtain sensitive information or access organisational systems by exploiting victims' positions.

These attacks are executed through deceptive messages designed to appear legitimate.

Best Practices and Preventive Measures

Ransomware Prevention Measures

1. Maintain regular backups of critical files on external storage devices or cloud platforms
2. Keep operating systems and software consistently updated to address security vulnerabilities
3. Install and maintain active antivirus software and firewalls
4. Exercise caution with suspicious email attachments
5. Download software exclusively from trusted sources



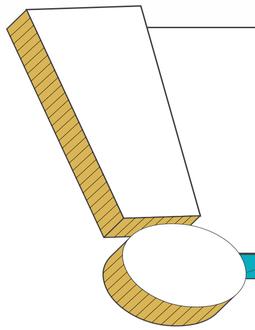
Warning!

Avoid replying to calls from unknown callers, often asking for personal or financial information as this is likely a fraud attempt.

Regular Account Monitoring

Regular financial account monitoring facilitates early detection and response to breaches through several measures:

1. Conduct periodic checks for unusual account activity
2. Opt for instant banking notifications
3. Report suspicious transactions immediately
4. Use authorized banking applications for account tracking
5. Regularly update security information is important to enhance account safety



Warning!

Avoid granting unnecessary permissions to mobile applications, as some may exploit these privileges to access your data.

Remote Working

Remote working enables employees to perform their duties from locations outside traditional offices whilst using technology to communicate and collaborate with colleagues and management.

Protection against Remote Working Security Risks

1. **Security Software Installation:** Ensure installation and regular updates of antivirus software and security programmes on your computer.

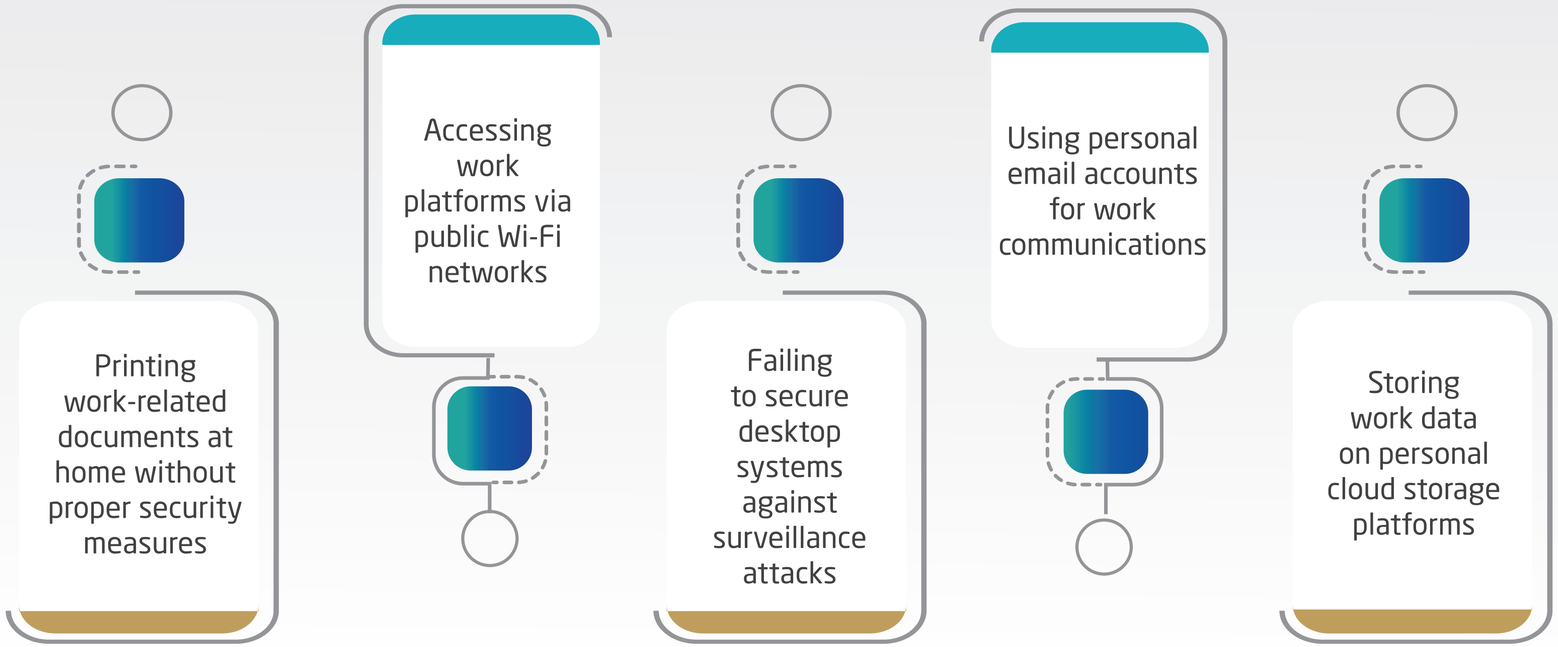
2. **Secure Network:** Implement protective services to shield work devices from various cyber threats.

3. **Software and Application Updates:** Regular updating of applications and security software eliminates security vulnerabilities present in legacy versions.

4. **Corporate Email Usage:** Strictly utilise work email accounts for business correspondence.

5. **Communication with IT Team:** Maintain contact with the IT department regarding security queries or suspected breaches.

Common Mistakes in Remote Working



Facts and Information

Ransomware has emerged as one of the most significant cyber threats to both corporations and government entities, resulting in substantial financial losses.

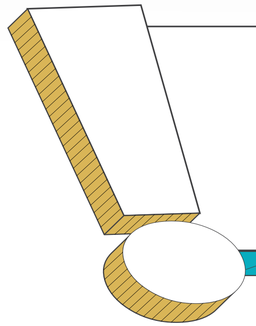
Data Security in Remote Working Environments

Utilise designated corporate email systems exclusively, avoiding personal email accounts

Store information on corporate-approved cloud storage platforms, refraining from personal cloud storage usage

Employ secure internet connections and VPN services when accessing public Wi-Fi networks

Implement two-factor authentication for password security



Facts and Information

Targeted cyber-attacks may remain undetected for months or even years, presenting ongoing systemic risks.

Responding to Ransomware Attacks

Isolate Infected Systems

Disconnect compromised devices from networks to prevent malware spread

Contact Relevant Authorities

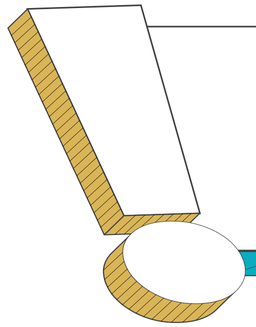
contact with official security bodies or appropriate cyber security companies

Avoid Ransom Payment

Don’t pay a ransom as this encourages criminal activity and may not guarantee file recovery

VPN Protection

1. Provide protection when using public network
2. Secures connections on public Wi-Fi
3. Prevents data infiltration and interception of data
4. Provides robust encryption for sensitive data
5. Protects against cyber-attacks on public networks



Facts and Information

The continuous enhancement of cybersecurity technologies is an absolute imperative for adapting to emerging and evolving threats in the digital world.

Email Security

1

Encryption

Converting data into unreadable format for protection.

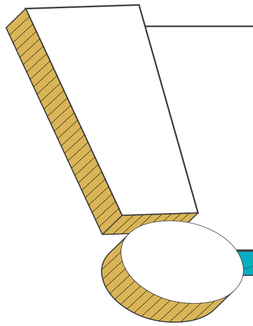
2

Encryption is crucial for email security; protecting data during transmission and ensuring only intended recipients can read it.

3

Available encryption methods

Utilising protocols such as SSL/TLS.



Warning!

Never ignore security notifications from applications or websites, as these alerts may indicate potential breach attempts.

Social Media Account Security

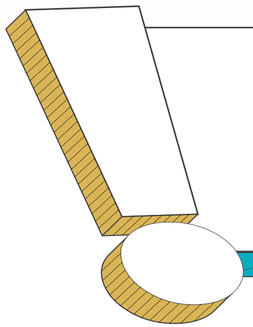
Password Security Enhancement can be done through:

01 Create strong passwords combining uppercase, lowercase, numbers, and symbols

02 Avoid obvious personal information in passwords

03 Regular password rotation

04 Enable two-factor authentication



Warning!

Avoid providing personal information in online surveys or competitions, particularly when the organising entity is unknown or untrustworthy.

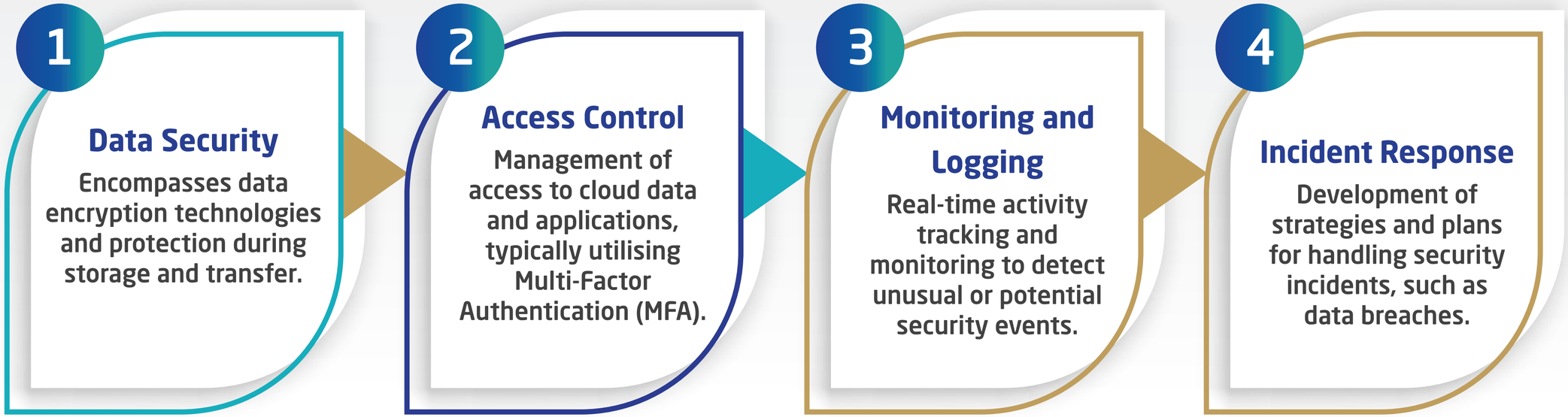
Privacy Settings Management

1. Regular review of social media privacy settings.
2. Control who can view your personal information.
3. Implement blocking for suspicious users.
4. Restrict public sharing of sensitive information such as addresses and phone numbers.

Cloud Security

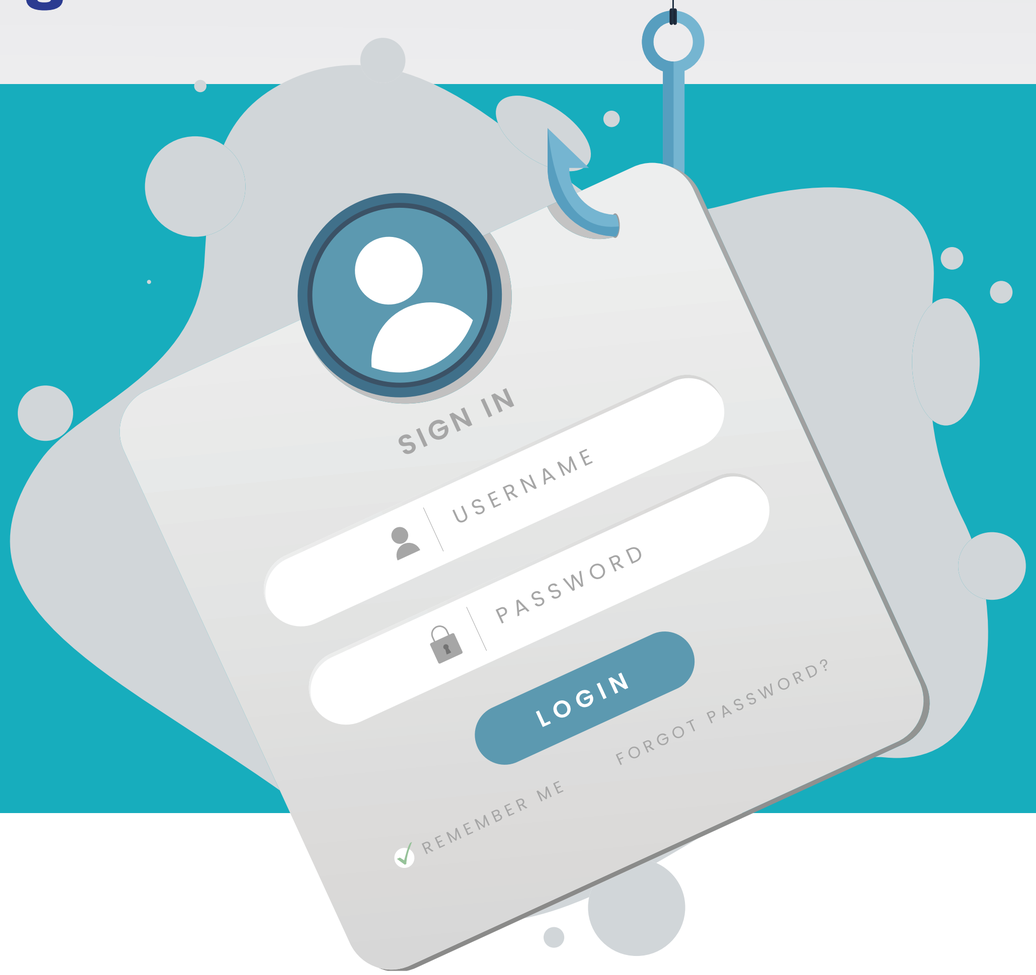
It is a set of comprehensive policies and technologies aimed at protecting cloud-based data, applications, and infrastructure. Cloud security aims at data security against internal and external threats.

Cloud Security Components



Password Management

Passwords serve as the first line of defence for protecting financial accounts and sensitive systems in the financial and banking sector. Effective password management significantly reduces the risk of cyber breaches.



Below are some best practices for managing passwords

01

Creating Strong Passwords

Use passwords that combine uppercase and lowercase letters, numbers, and symbols.

Avoid common words or personal information, such as names or birth dates.

02

Regularly Changing Passwords

It is advisable to change passwords every 60-90 days to minimise the risk of breaches.

03

Avoiding Password Reuse

Avoid reusing the same password for multiple accounts, particularly for financial accounts.

04

Using Password Managers

Employ password management software to securely store and organise passwords.

05

Enabling Two-Factor Authentication (2FA)

Add an extra layer of security by linking accounts to SMS messages or authentication apps.

06

Avoiding Password Sharing

Refrain from sharing passwords with others and avoid writing them in insecure locations.

07

Being Cautious of Phishing Attacks

Avoid clicking on suspicious links or attachments that prompt you to enter your passwords.

Facts and Information

- Over 80% of cyberattacks result from weak or reused passwords.
- Password managers can generate random passwords and secure them with strong encryption.

Conclusion

Digital safety is a shared responsibility that requires awareness and vigilance. These slides summarise key practices and measures for protecting the financial and banking sector from cybersecurity threats, with an emphasis on continuous prevention and the enhancement of security systems.

Adhering to these guidelines reduces the possibility of breaches, safeguards sensitive data, and ensures the secure and confident operation of financial activities, thereby bolstering the stability of the financial sector in the face of digital challenges.

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:

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency