الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Target Audience

Women and Families

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

Women and Families

Teacher's Guide

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

January 2025
Doha, Qatar

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

To Contact 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.

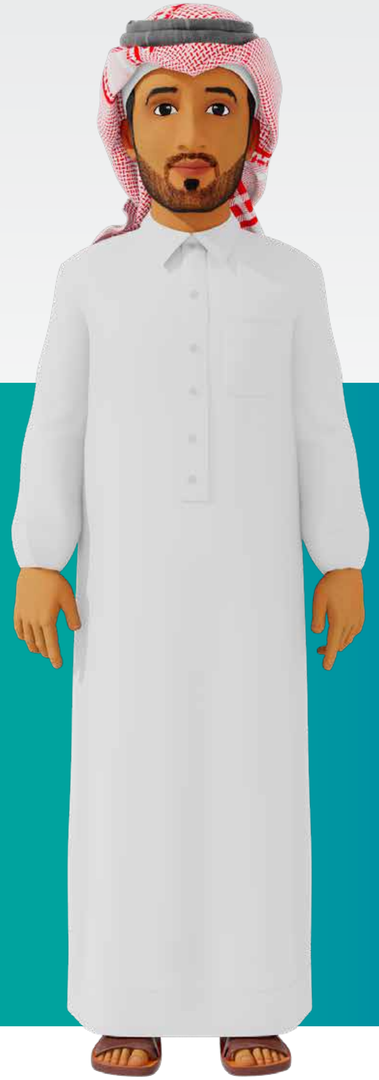
These efforts are part of the National Initiative for Digital Safety, organised by The National Cyber Security Agency, to establish a secure digital environment for all members of society.

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:

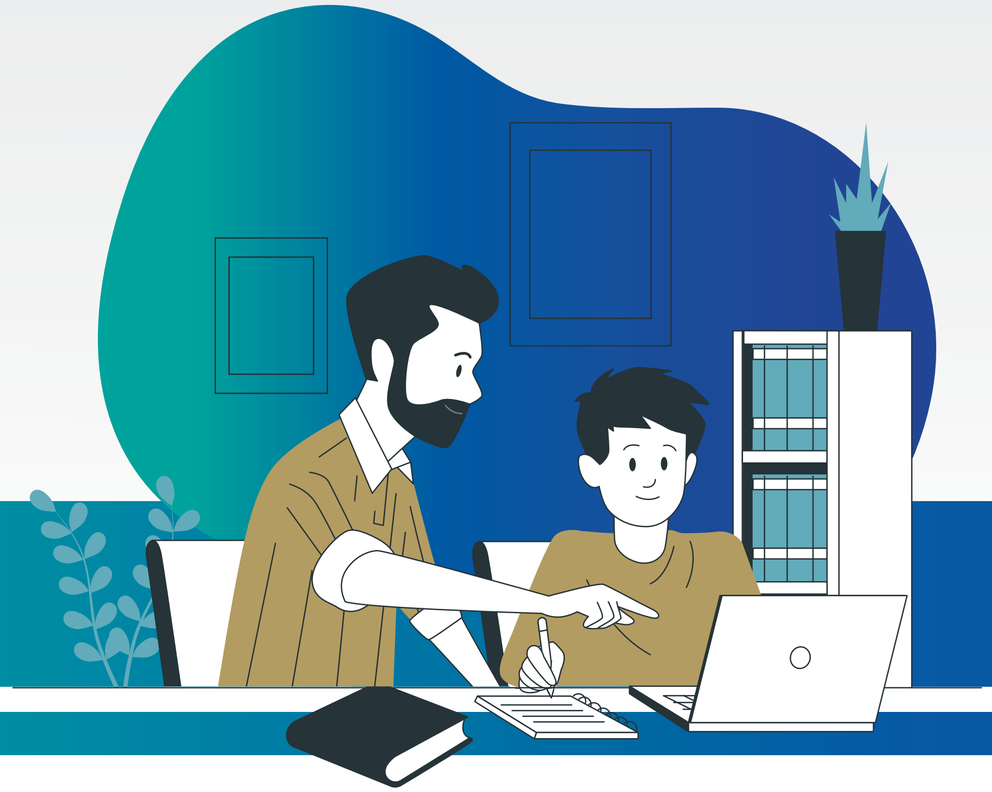
- Senior Citizens
- Women and Family
- People with Special Needs
- University Students
- Expatriate Workers
- Civil Society Organizations
- Financial and Banking Sector

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



Digital Security for Parents

Personal Data

Data

It refers to any information or facts that can be collected and analysed, including numbers, texts, images and others. Data plays a major role in decision-making and technology development.

Personal Data

This includes any information that can identify an individual, such as their name, address, phone number, email, financial details or IP address.

Examples of Personal Data

01 National identification number

02 Medical and health information

03 Bank account information

04 Online activities

Digital Identity Theft

Digital identity theft occurs when an unauthorised person accesses someone else's identity information online and uses it illegally for personal or financial benefit. Such information may include personal account details, passwords, or financial information.

Examples of Stolen Data

- Credit card numbers
- Passwords
- Social security or national ID numbers
- Bank information

How Digital Identity Theft Occurs?

01

Phishing

Victims are tricked into disclosing sensitive information through fake messages or websites that seem legitimate.

02

Malware

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

03

Database Breaches

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

04

Brute Force Attacks

Attempting to hack accounts by trying millions of possible password combinations.

Consequences of Digital Identity Theft

Financial Losses

Criminals can use stolen data to withdraw money from bank accounts or make fraudulent purchases.

1

Forgery

The use of stolen identity for illegal activities, such as signing contracts or opening new accounts in the victim's name.

2

Reputational Damage

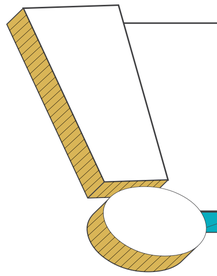
The stolen identity may be used for illicit activities, harming the victim's reputation.

3

Risks of Digital Identity Theft

Digital identity theft is a major risk for online users, involving the unlawful acquisition of someone else's personal information. Protection against this threat can be achieved by:

- Limiting personal information published online.
- Using strong, regularly updated passwords.
- Avoiding links in emails from unknown sources.



Facts and Information

Securing personal data online requires following security practices, such as using strong passwords and updating applications regularly.

Phishing

A type of cyberattack where attackers use fake emails or websites to trick people into revealing sensitive information, such as passwords or bank account details.

How Does Phishing Works?

01 Fraudulent Emails

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

02 Fake Websites

The email contains a link to a fake website resembling the original, where the victim is asked to enter personal information.

03 Exploiting Information

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

Online Donations and Phishing

Online donation requests may serve as phishing tools. To avoid them, follow these tips:

01 Verify the charity's website for clear information on donation methods, contact details and address.

02 Confirm the charity is officially registered with relevant entities, such as Qatar's Charitable Affairs Authority.

03 Avoid donations via bank transfers and ensure that online donations are made through pages that start with "https".

Online Donations and Phishing

04 Avoid cryptocurrency donations, as these may indicate fraud.

05 Check your bank account after donating to confirm only the specified amount was deducted and keep a donation record.

06 Be cautious of appeals with minimal details or promises of prizes or rewards in exchange for donations.

Signs Indicating Device Breach

01 Receiving email notifications of login attempts to accounts, despite not attempting to log in.

02 Device slowing down, heating up, and delays in responding to commands.

03 Pop-up windows displaying annoying messages.

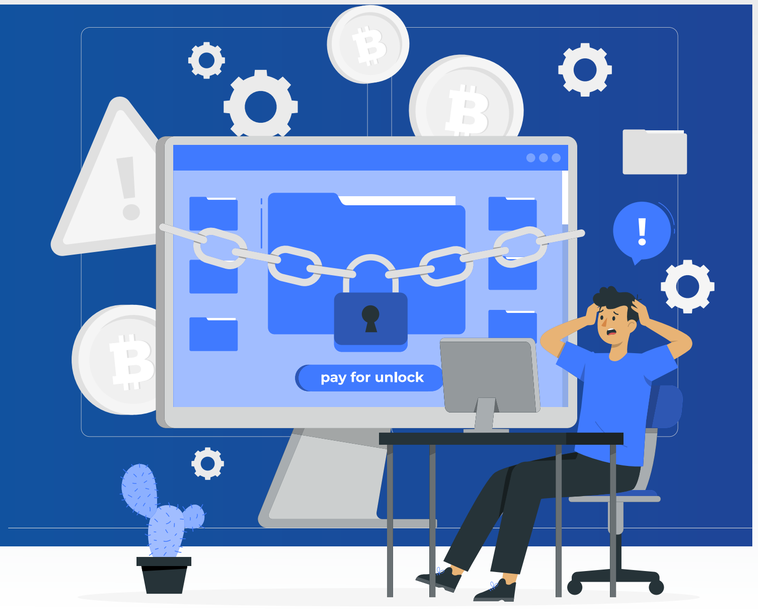
04 Browser windows, tabs, or applications on your device opening by themselves.

05 Receiving unsolicited emails in your inbox.

06 Frequent redirection to unwanted websites.

Ransomware

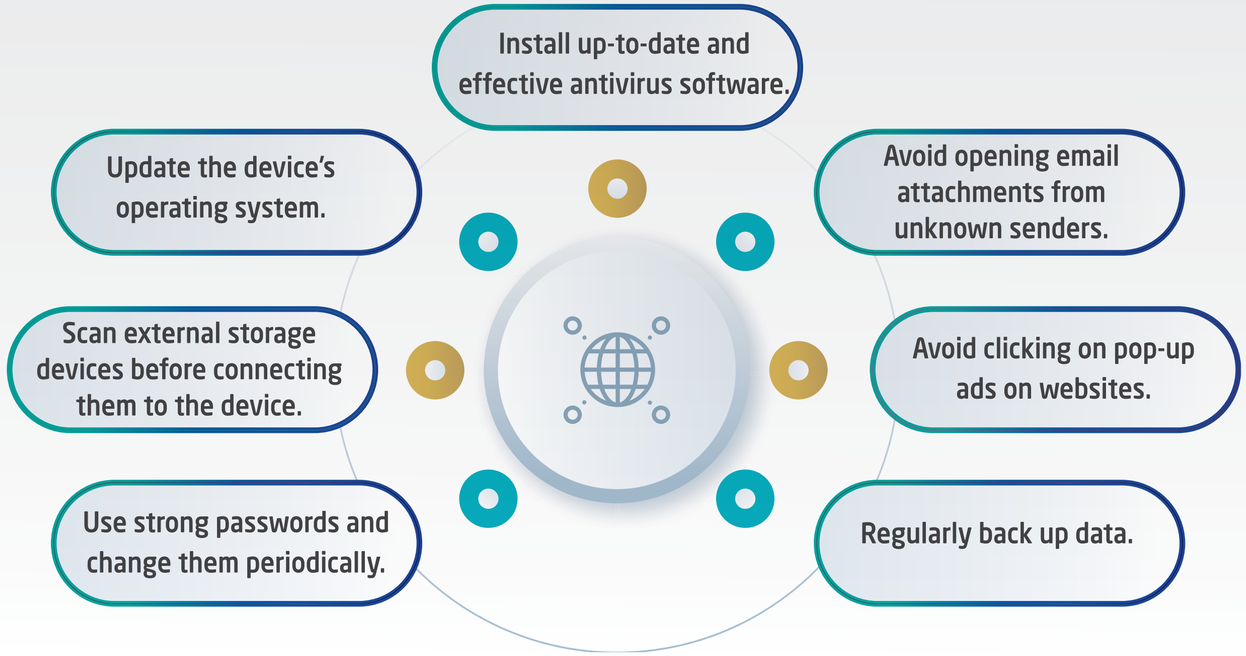
- Ransomware is a type of cyberattack targeting individuals and organisations.
- Ransomware attacks encrypt data, preventing users from accessing it unless a ransom is paid.
- If the ransom is not paid, the attacker may destroy the data.



Warning!

Avoid downloading antivirus or security software from unofficial sources, as these may contain malicious software.

Protection Against Ransomware



Warning!

Avoid responding to text messages requesting personal or financial information, as these are often part of fraudulent schemes.

Cyberbullying and Strategies to Protect Children

- Cyberbullying is one of the most serious challenges children face in the digital world, often causing long-term psychological and social harm.
- It typically involves posting negative comments, offensive images, or harassing messages to upset or embarrass children online.

Strategies to Protect Children from Cyberbullying

Raising Awareness

Teach children how to recognise cyberbullying and encourage them to speak up if they experience it.

Monitoring and Guidance

Keep track of children's online activities in a friendly manner while guiding them to use platforms safely.

Privacy Settings

Adjust privacy settings on social media to limit unwanted access.

Avoiding Responses

Instruct children not to respond to offensive messages and to block disruptive accounts.

Strategies to Protect Children from Cyberbullying

Documenting Evidence

Save evidence of cyberbullying (e.g., screenshots) to report incidents to the appropriate authorities.

Seeking Professional Help

Consult counsellors or mental health experts if the child's emotional well-being is affected.

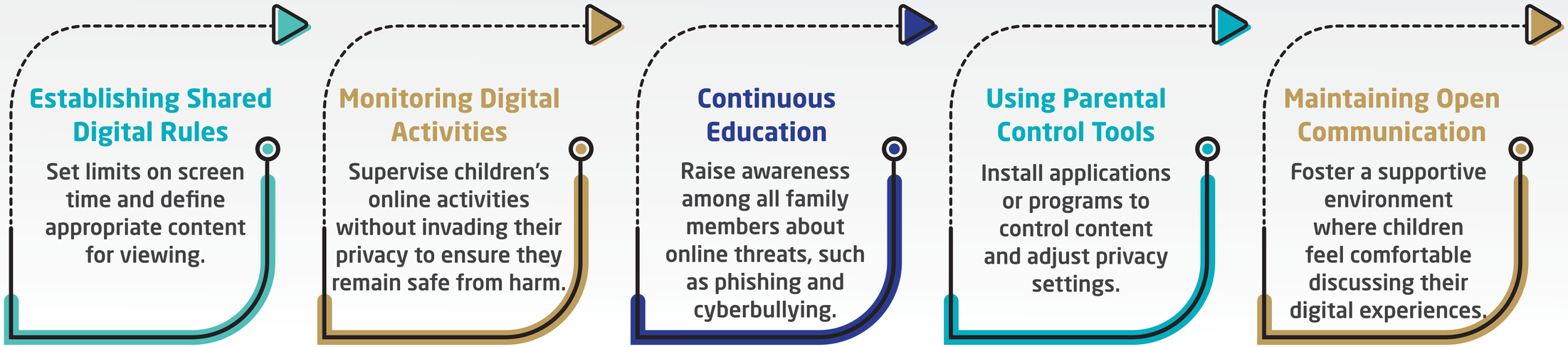
Using Protective Software

Install parental control programs that monitor activities and minimise risks.

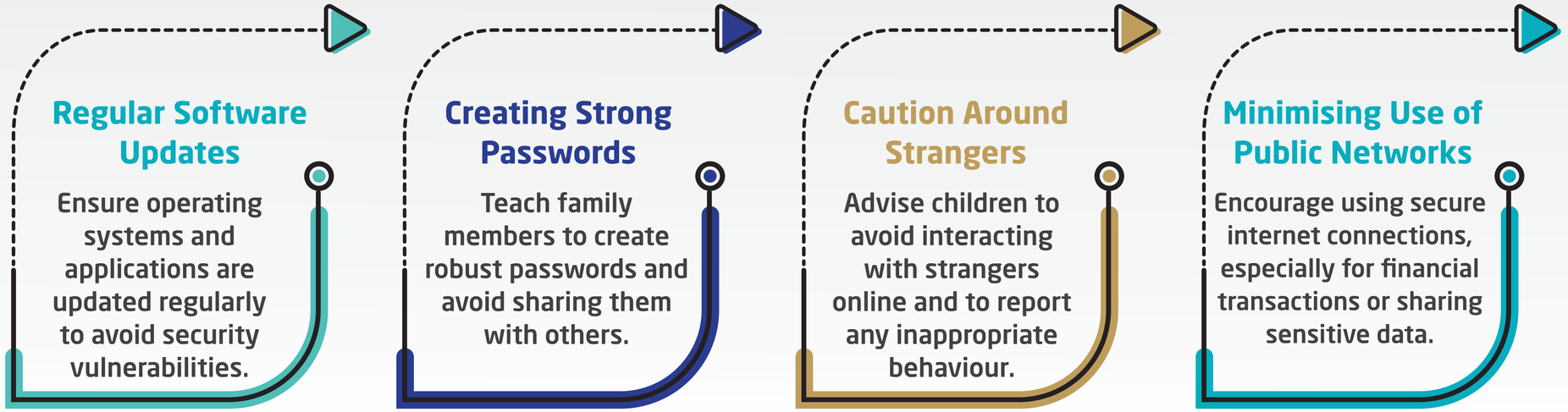
Safe Digital Habits for Families

In an era of rapid digital advancements, practising safe digital habits has become essential to ensure the safety of families and protect them from online risks. These habits promote responsible and secure use of technology for all family members.

Key Safe Digital Habits for Families



Key Safe Digital Habits for Families



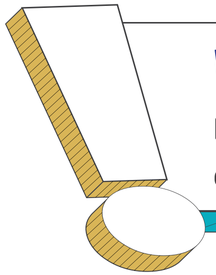
Digital Security for Children

Common Mistakes Leading to Online Fraud

- Browsing on public Wi-Fi without using a Virtual Private Network (VPN).
- Oversharing personal information on social media.
- Using similar passwords for multiple online accounts.
- Not enabling automatic software updates increases the risk of virus infiltration.

Common Mistakes Leading to Online Fraud

- Clicking on links in emails without verifying their reliability.
- Responding to emails offering gifts and prizes without verifying them.
- Ignoring basic security features like two-factor authentication.
- Shopping online through unreliable websites.



Warning!

Be cautious of messages that urgently request sensitive data or claim to be from official entities requesting personal information.

Safe Browsing Rules

1. Install up-to-date antivirus software.
2. Avoid opening pop-up ads on web pages.
3. Download software and apps only from trusted websites.
4. Avoid making purchases through untrusted e-commerce sites.
5. Create strong passwords and change them regularly.
6. Do not open email attachments from unknown senders.
7. Enable the firewall.

Protecting Personal Information

Avoid sharing personal information

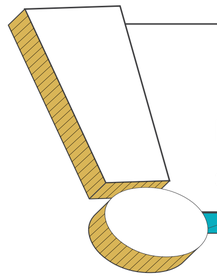
Refrain from sharing sensitive data online.

Use trusted security software

Use reliable antivirus and anti-spyware programmes.

Regularly update software and systems

Update software regularly to close security gaps.



Facts and Information

Reports from cybersecurity firms show that the frequency of global cyberattacks is doubling annually, highlighting the need to strengthen security measures.

Two-Factor Authentication

Two-factor authentication (2FA) is an additional security layer to protect personal accounts. Instead of relying solely on a password, 2FA adds a second step to verify the user's identity, making it harder for hackers to access accounts even if they manage to steal the password.

How It Works

Two-factor authentication is achieved by combining two elements:

* **1. Something you know (your password)**

  This is entered upon logging in.

* **2. Something you have (a temporary code or device)**

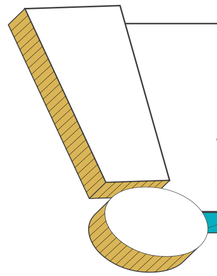
  This could be a code sent to your mobile phone or an authentication app.

Importance of Two-Factor Authentication

Two-factor authentication enhances the security of your devices and personal data.

Two-factor authentication requires more than just entering a password to access your accounts.

2FA may also involve logging in using fingerprint, eye, or facial recognition, or confirming with a mobile phone number.



Warning!

Avoid clicking on unknown or suspicious ads while browsing the internet, as they may lead to harmful websites or result in data theft.

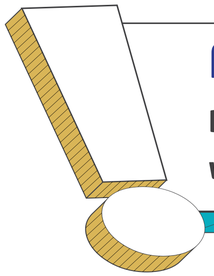
Privacy Settings

Most online services offer settings to control aspects such as:

Who can view what you post, as seen on social media platforms, allowing you to share with friends only, friends of friends, or the public.

Restricting specific posts to a selected group of people, such as family members, allows you to make your posts public or private.

Privacy settings on smartphones help restrict access to your location, contacts and personal information.



Facts and Information

Distributed Denial of Service (DDoS) attacks have increased significantly recently, causing widespread disruptions to websites and digital services.

Digital Identity and Password Security

To safeguard digital identity, strong passwords are essential.

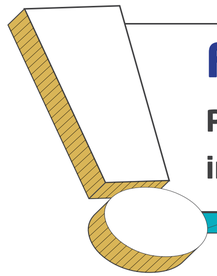
01 Create strong, hard-to-guess passwords, and use a password manager to store them securely.

02 Choose passwords that combine letters, numbers and symbols.

03 To add another security layer, enable two-factor authentication.

04 Avoid reusing any password for multiple accounts or services.

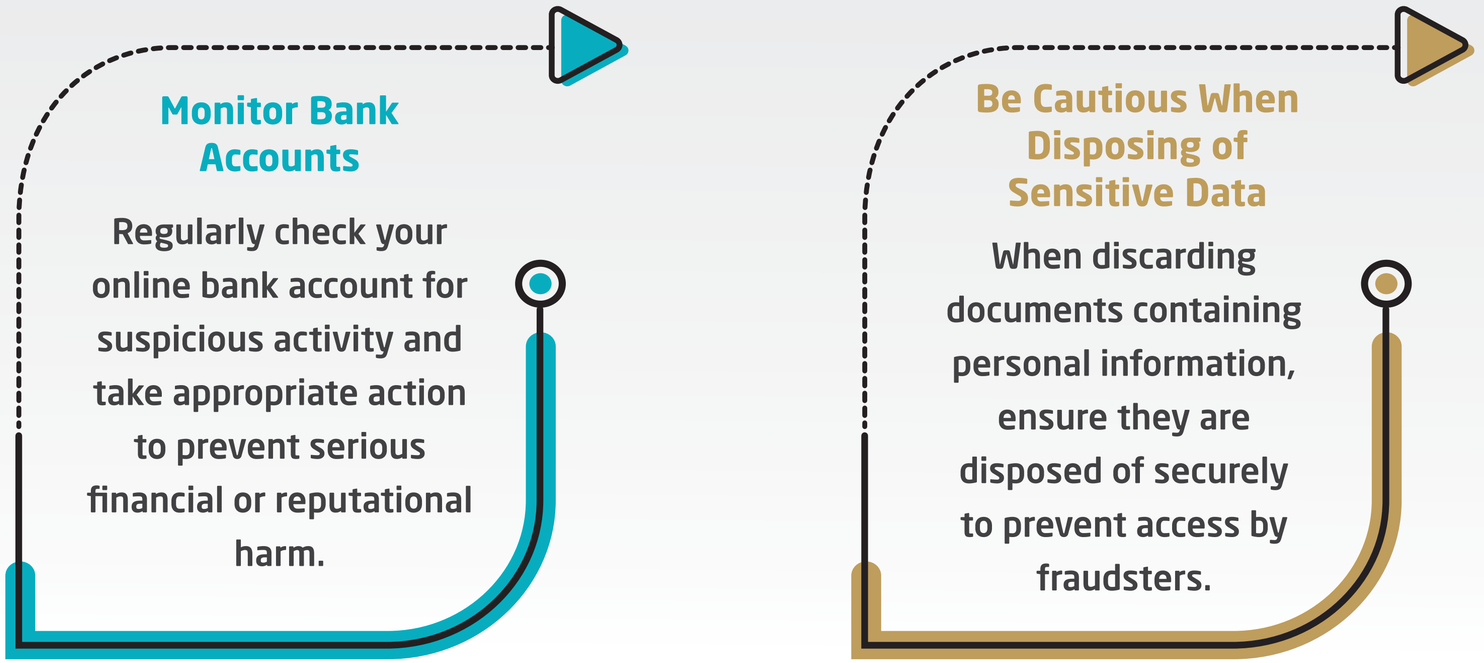
05 Regularly update passwords.



Facts and Information

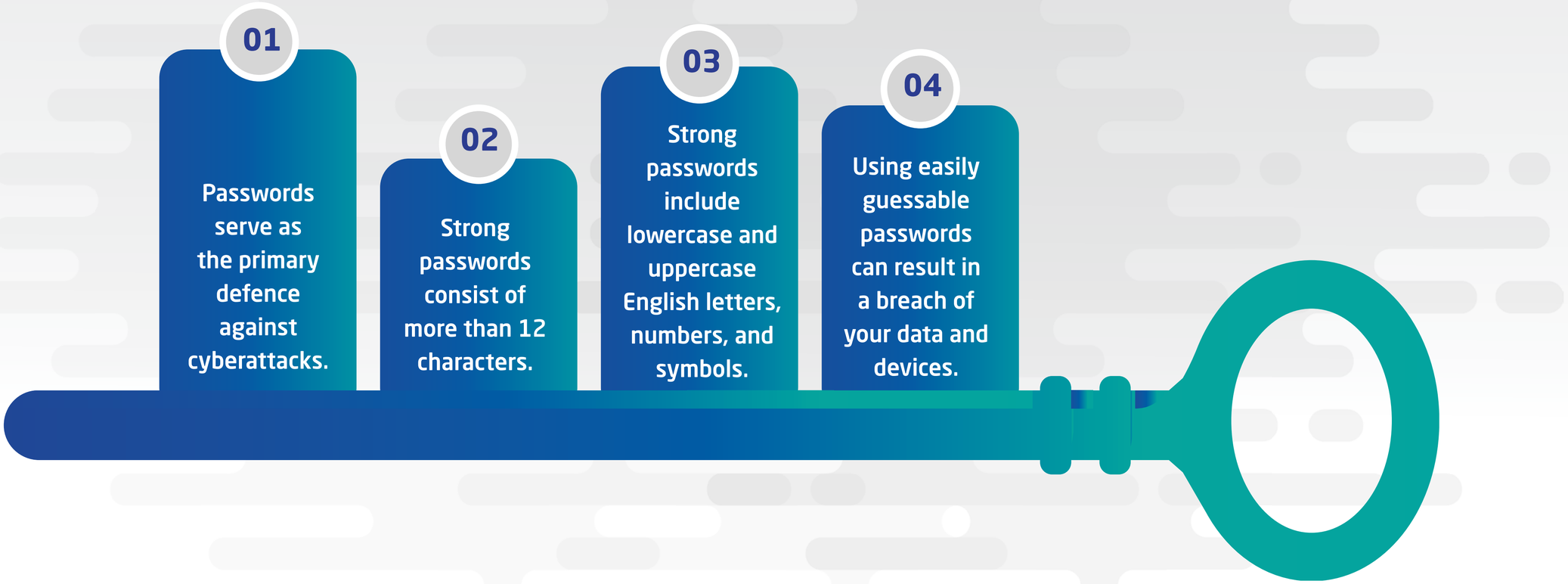
Phishing is one of the most common attacks, deceiving users into providing personal information through fake messages.

Digital Identity Protection Measures



The same precaution applies to computers and phones. Before selling a device to upgrade, confirm that all personal data has been completely erased.

Passwords

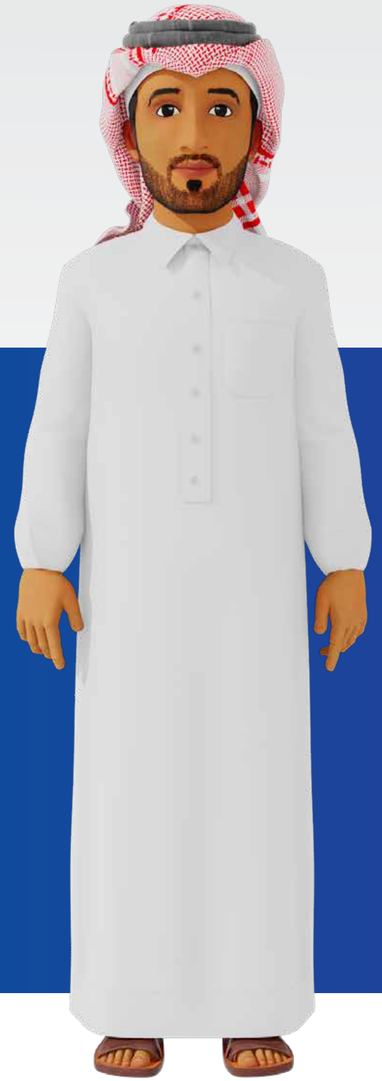

01
Passwords serve as the primary defence against cyberattacks.
02
Strong passwords consist of more than 12 characters.
03
Strong passwords include lowercase and uppercase English letters, numbers, and symbols.
04
Using easily guessable passwords can result in a breach of your data and devices.

Conclusion

Digital safety is a shared responsibility that demands awareness and vigilance. Enhancing the digital security of the family requires adhering to straightforward practices, including securely managing passwords, protecting personal data, preventing cyberbullying and dealing with phishing attacks. These actions form fundamental steps in safeguarding the family from the increasing 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 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