

Securing electronic devices and countering security breaches

Presentation Slides

Training Kit



CyberEco

معا لدعم السلامة الرقمية
Together to support digital safety



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property rights

The National cybersecurity Agency in the State of Qatar owns the work, and copyright, publishing, printing rights, and all other intellectual property rights are protected by The National cybersecurity Agency in the State of Qatar.

As a result, the Agency retains all rights to these materials, and it is prohibited to republish, quote, copy, or transfer them in whole or in part in any form or by any means whether electronic or mechanical, including photographic reproduction, recording, or the use of any information storage and retrieval system, whether existing or invented in the future, unless the agency has given written permission.

Anyone who breaks this could face legal consequences.

December, 2023

Doha, Qatar

This content is produced by the team of
National Cybersecurity Excellence Management, National Cyber Security Agency.

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ cyberexcellence@ncsa.gov.qa

☎ 00974 404 663 78

☎ 00974 404 663 62

Workshop Time Table

Content	Allocated Time
General Introduction	10 minutes
The theoretical aspect	30 minutes
Educational Videos	30 minutes
Short Break	20 minutes
Dialogue and Discussion with Students	30 minutes
Total training time	2 hours

The Scientific Content Index of the training package

Chapter One

The Significance Of Electronic Device And Network Security.....5

The Significance of digital stability for networks and connected devices.....6

Digital threats in digital devices (phone, computer).....12

Chapter Two

Types of digital threats in devices.....14

Ransomware attack.....15

Device data theft.....19

Unauthorized access.....27

Malware.....31

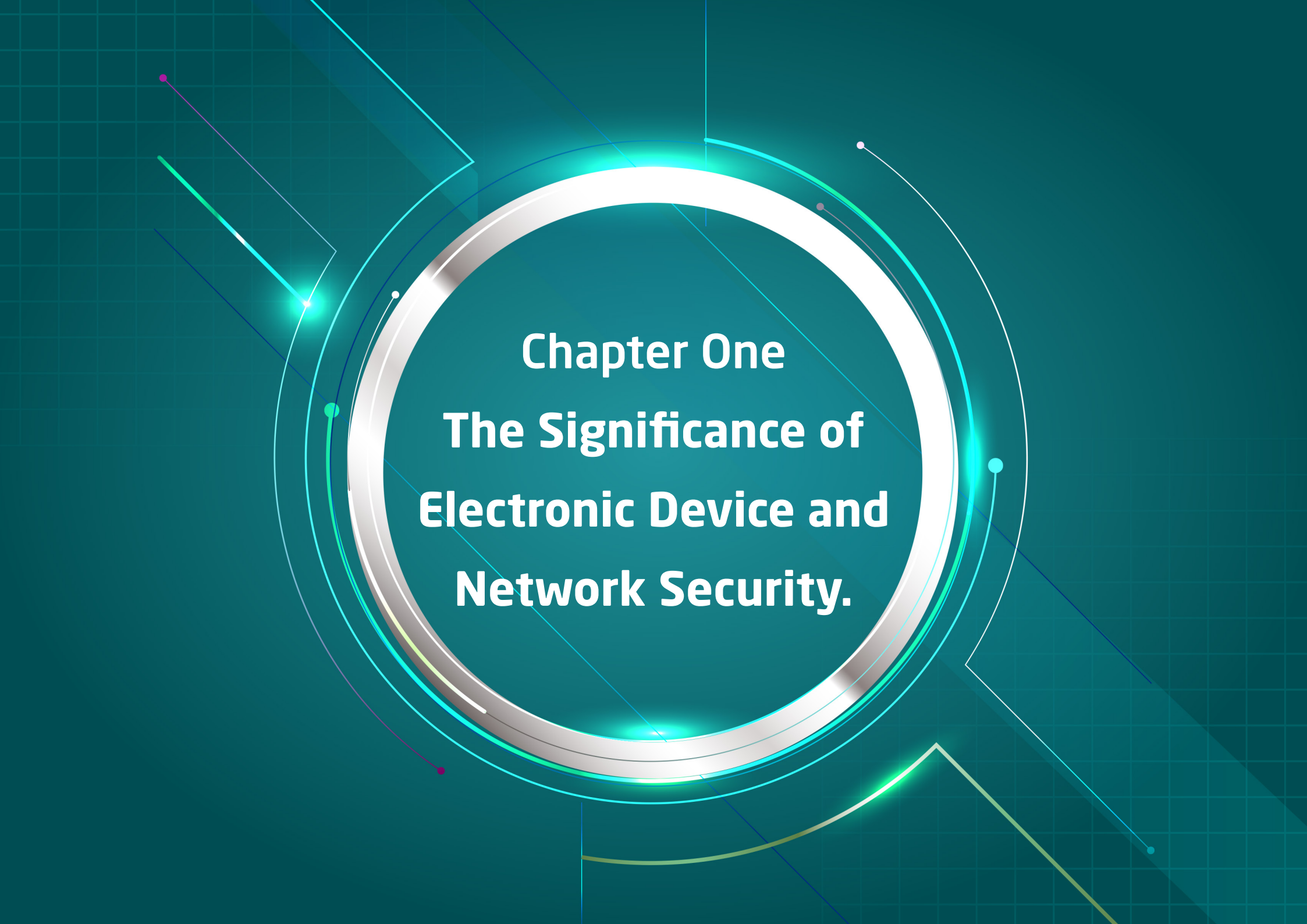
Chapter Three

How to Secure Devices from Digital Threats.....37

Passwords.....38

Data backup.....44

Training Cards.....46



Chapter One
The Significance of
Electronic Device and
Network Security.

First

The Significance of digital stability for networks and connected devices



Information security

It refers to the means, tools, and procedures necessary to ensure the protection of information from internal and external threats. It is the discipline that studies how to provide confidential and secure protective measures for information and how to counteract attacks on it.



Information security relies on several steps to ensure the protection of devices and networks from unauthorized access. These include

01

Utilizing the username and password.

02

Securing the computer from hackers using antivirus software.

03

Securing software, data, and backups.

04

Utilizing a firewall.

Network Security

It is part of the information security system that focuses on securing the use and integrity of the network, and consequently, the integrity of data. This field encompasses both hardware and software technologies. Network security targets and prevents a diverse range of threats from entering or spreading within your network.



Fundamentals of Network Security

- Access Control, It refers to enforcing security policies that prevent unauthorized users from accessing and, consequently, gaining entry to your devices, and data. This process is referred to as 'network access control'.
- Antivirus and anti-malware programs.
- Application Security.

- Behavioural analysis tools automatically distinguish suspicious activities for prompt processing.
- Data Loss Prevention.
- Email Security.
- Firewalls.
- Intrusion Prevention Systems.
- Mobile Device Security.
- Network Segmentation.
- Web Security

Digital threats in digital devices (phones, computers)

01 Data leakage

Sometimes, mobile device applications can unintentionally lead to data leakage. For example, free “malicious” apps can be a real problem for mobile users who grant them comprehensive permissions without always checking security.

02 Network spoofing

Public Wi-Fi networks are often insecure, and to protect against electronic attacks, users should rarely use free Wi-Fi on their mobile devices and should never use it to access sensitive or personal services, such as banking information or credit card details.

Digital threats in digital devices (phones, computers)

03 Phishing Attacks

Users of mobile devices are more vulnerable to attacks, often being the first recipients of seemingly legitimate email messages and falling for the bait. Thus, it is crucial never to click on unfamiliar email links.

04 Spyware

To protect devices from it, it is essential to download an effective suite of antivirus and anti-malware programs and eliminate them before they have the opportunity to collect your personal data.

The image features a dark teal background with a subtle grid pattern. A large, glowing circular element is the central focus, composed of multiple concentric rings. The innermost ring is a bright, metallic silver, while the outer rings are a vibrant cyan with a soft glow. Several thin, colored lines (purple, green, blue) extend from the center towards the corners, ending in small dots. The text is centered within the silver ring.

**Chapter Two:
Types of digital
threats in devices**

Ransomware attack

These are malicious programs designed to prevent users or enterprises from accessing files on their computer devices, demanding a ransom in exchange for restoring access to their files.



How ransomware operates

Infection vectors and dissemination

Ransomware operators frequently employ phishing emails as a delivery method. These malicious emails may contain links to websites that host harmful downloads or attachments.

Data encryption

Once cybercriminals gain access to a computer system, whether for an individual or an enterprise, the system begins encrypting its files and replacing the original versions with encrypted ones to later ransom them.

Ransom demand

Once the file has been encrypted, the ransomware is ready to deliver a ransom demand.

How to protect against ransomware

- Cybersecurity awareness training and education
- Regular data backup.
- Patching vulnerabilities in systems that have not yet been patched.
- User authentication mechanisms serves as a crucial countermeasure to protect against the exploitation of compromised or stolen passwords.
- Reducing the attack surface through addressing

Phishing messages.

Unpatched vulnerabilities.

Remote access solutions.

Mobile malware.

How to mitigate active ransomware infections

01

Isolating the device

It is crucial to isolate the infected device from other connected devices to prevent the malware from spreading.

02

Maintain the computer in an operational state

File encryption can render a computer unstable, so shutting down the computer is not a guaranteed solution, as it may result in memory loss.

03

Creating a backup.

04

Ensure the availability of decryption tools

Check the No More Ransom Project to see if a free decryption tool is available to help you recover your files.

05

Seek assistance

A specialist can assist in recovering these copies if they haven't been deleted by malware.

06

Reformat and Restore

Recover the device using a previously saved clean backup or reinstall the operating system to ensure that the malware is completely removed from the device.

Device data theft



Definition of Data Theft

It involves the unlawful transfer or storage of personal, sensitive, or financial information. This can encompass passwords, source code, algorithms, processes, or proprietary technologies. It constitutes a grave breach of security and privacy.



Data theft is also known as a 'data breach' or a 'data leak', but there are nuanced distinctions between these concepts. These are:

01 Data leaks

occur when sensitive information is inadvertently revealed, either online or via misplaced or lost hard drives or devices. This implies that cybercriminals can acquire unauthorized access to sensitive data without exerting any effort.

02 Data breaches

refer to deliberate cyberattacks.

How does data theft occur?

Data theft can be perpetrated using a diverse range of tools.

Social engineering

The most common form is phishing, occurring when the attacker disguises themselves as a trusted entity to deceive the victim into opening an email, text message, or instant message.

1

2

Weak Passwords

System Vulnerabilities

Security vulnerabilities assist hackers in exploiting them to steal data, and outdated antivirus programs also lead to the creation of security vulnerabilities.

3

4

Internal Threats

Employees within an enterprise may possess access to customers' personal information, which could be exploited.

How does data theft occur?

Human error

It involves sending sensitive information to the wrong person, inadvertently emailing to an incorrect address, or delivering a physical file to an unauthorized individual.

5

Installing software from unsecure sources
Acquiring software or data from compromised websites, such as those plagued by viruses.

6

Theft or loss of electronic devices.

7

Publicly Available Information

Many pieces of information can be discovered through online search operations and by examining user posts on social media platforms.

8

What types of data are typically stolen?

Customer records.

1

2

Financial data, such as credit card or debit card information.

Source codes and algorithms.

3

4

Descriptions of ownership processes and operational methodologies.

Network credentials, such as usernames and passwords.

5

6

Human resources records and employee data.

7

Private documents stored on computers.

Data theft consequences

Potential legal claims from clients whose information has been disclosed.

1

Ransom demands from attackers.

2

Recovery costs, such as restoring or patching compromised systems.

3

Defamation and loss of customers.

4

Fines or penalties from regulatory bodies depending on the industry.

5

Interruptions during data recovery.

6

7

For individuals whose personal information has been breached, the primary consequence is the potential for identity theft, which can result in financial losses and emotional distress.

How to keep data secure

1

Utilize strong passwords.

2

Avoid utilizing the same password for multiple accounts.

3

Avoid writing down your passwords anywhere.

4

Multi-Factor Authentication

5

Exercise caution when sharing personal information

6

Limiting the sharing on social media platforms.

7

Close inactive online accounts.

8

Update your systems and software regularly

9

Be careful of free Wi-Fi services.

10

Utilize Antivirus programs.

Unauthorized Access (Illegal Access)

Unauthorized access involves gaining entry to computer resources without authorization. These resources may include a system, network, program, or data. Unauthorized access is typically perpetrated by hackers, but can also occur unintentionally. Individuals with legitimate access to the system may inadvertently encounter insecure files that were not intended for their perusal.



How unauthorized individuals gain access to systems and files

1

The user inadvertently guessing the password for sensitive files or data.

2

Perpetrating sophisticated attacks that require meticulously planning over several weeks, and may even involve espionage operations targeting enterprises and their users.

3

Cybercriminals can go even further in their deception to gain enough trust to appear as authorized individuals.

The risks of unauthorized access

Disruption of electronic systems.

1

2

Causing harm to the target; unauthorized data is typically sensitive and can cause distress or damage to the victim.

Data theft for ransom purposes.

3

4

Causes material damage to network-connected devices.

Defaming enterprises and individuals.

5

6

Financial and reputational penalties for enterprises exposing customers to harm.

7

The escalating costs due to patching vulnerabilities and issues arising from unauthorized access to systems and files, as well as compensating affected parties.

Tips for detecting and preventing unauthorized access.

01

Setting a strong and complex password.

02

Regular prompts and verifications concerning cybersecurity procedures through training.

03

Reducing the number of devices that can access sensitive data.

04

Securing all endpoints by installing antivirus software on each endpoint to remove and detect malware.

Malware

Malware It is a comprehensive term that describes any malicious software or code that damages systems. Deliberately seeking to invade computer devices, systems, networks, tablets, and mobile devices, it aims to damage or disable them, often by partially controlling device operations.



How can I determine if I am infected with malware?

- Your computer is performing poorly.
- The appearance of disruptive advertisements on the screen.
- Your system crashes, manifesting as freezing or the infamous Blue Screen of Death (BSOD), the latter occurring on Windows systems after encountering a severe error.
- Mysterious loss of disk space.
- An unusual increase in internet activity for your system.
- Browser settings automatically change.
- The antivirus program stops working, and you can no longer restart it.
- Losing access to your files or the entire computer.

Types of malware

1

Adware.

2

Spyware.

3

Viruses.

4

Worms.

5

Trojans.

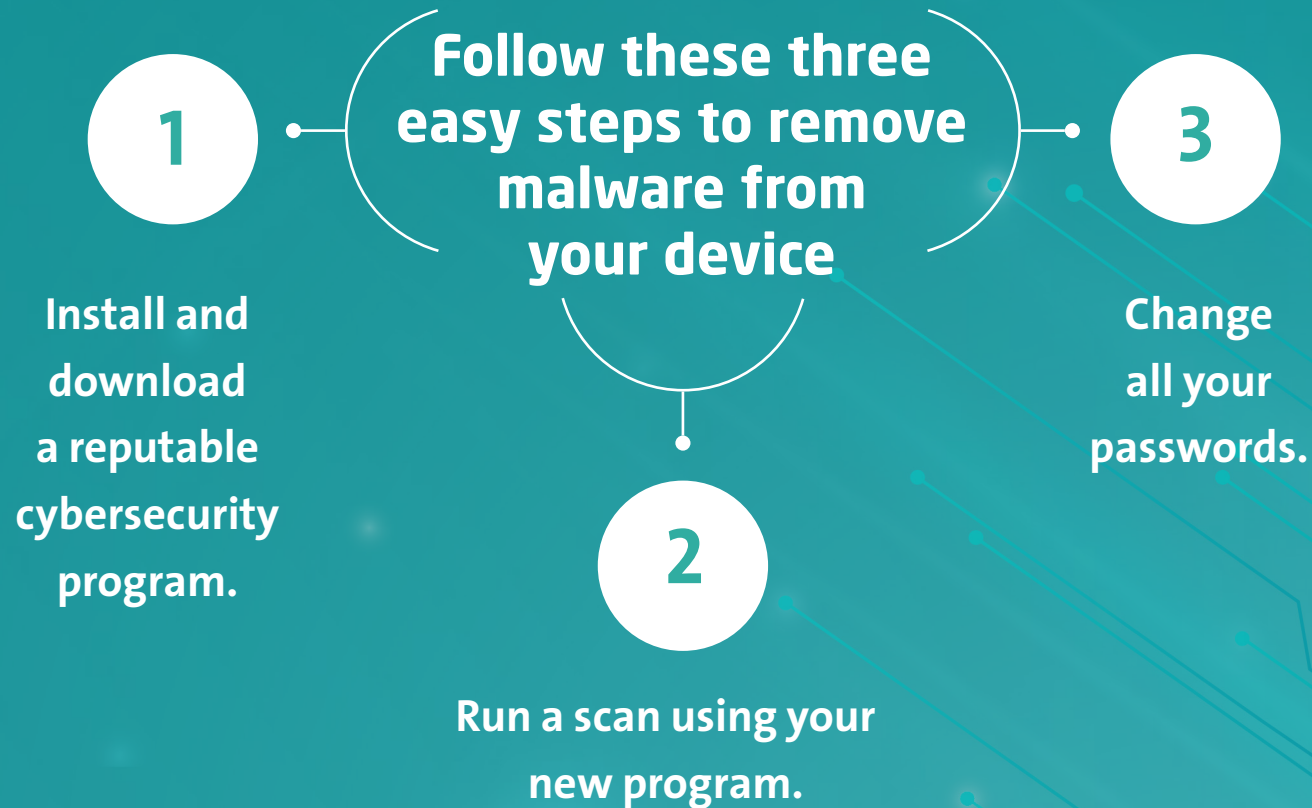
6

Ransomware.

7

Exploit.

How to remove malware



How to protect against malware.

- Be cautious and attentive if the website is not a top-level domain, such as com, mil, net, org, edu, or biz, for example, among others.
- Use strong passwords with multi-factor authentication.
- Avoid clicking on pop-up ads while browsing the Internet.
- Avoid opening email attachments from unknown senders.
- Do not click on suspicious links.
- Do not download programs from untrustworthy websites..

- Adhere to official applications from Google Play and the App Store.
- Ensure that your operating system, browsers, and add-ons are patched and up to date.
- Remove any programs that you no longer use.
- Regularly create a backup of your data.
- Download and install a cybersecurity program that scans for threats and prevents them from accessing your device.

The image features a dark teal background with a subtle grid pattern. In the center, a large, glowing circular ring with a metallic, reflective finish is the focal point. The ring is surrounded by several concentric, glowing lines in shades of cyan and blue. Various geometric shapes, including triangles and lines, extend from the center towards the corners, some ending in small colored dots (pink, green, blue). The overall aesthetic is clean, modern, and high-tech.

Chapter Three
How to Secure
Devices from Digital
Threats

Passwords



What is password protection?

Password protection helps secure your data from malicious actors by detecting and blocking known weak passwords and terms associated with you. It is an access control technique that assists in securing sensitive data from infiltrators, ensuring that access is only possible through the use of correct credentials.



The Significance of Password Protection

It serves as the first line of defense against unauthorized access to accounts, devices, and files online. Strong passwords help secure data from malicious entities and malware. The stronger the password, the greater the protection of information.



The Consequences of Weak Passwords

For individuals, the loss of personal information can have financial and long-term reputational consequences.

When cybercriminals gain unauthorized access to enterprise data, it can result in significant revenue loss, intellectual property compromise, operational disruptions, regulatory fines, and defamation.



General Guidelines for Creating Strong Passwords

1

Use a minimum of
12 characters.

2

Use a combination
of letters, numbers,
and symbols.

3

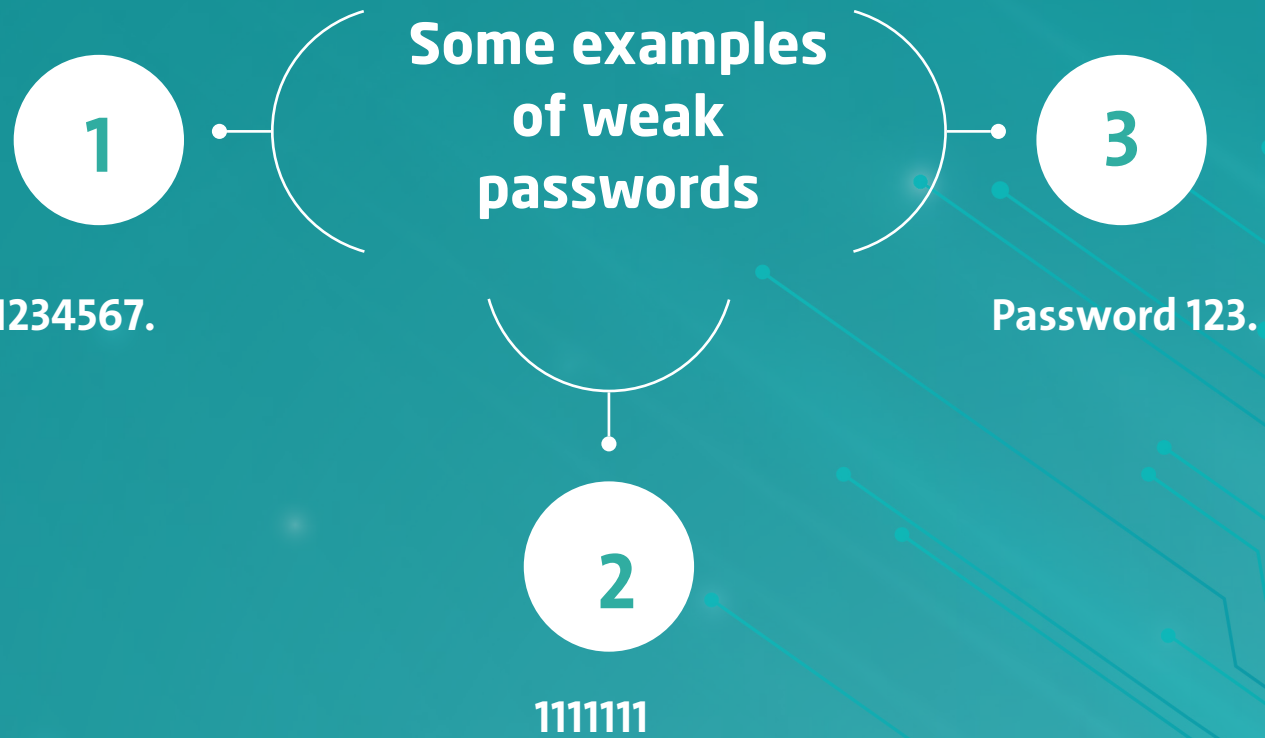
Use at least one
uppercase letter.

4

Use a different password for
each of your accounts.

5

Use uncommon and
unconventional words, such
as song lyrics, quotes, or
common phrases.



Data Backup

Effective Strategies for Safely Backing Up Your Data

➤ 1-2-3 rule refers to creating 3 different copies of data, placing them on two different types of storage devices, and keeping one copy off-site.

There are several ways to achieve this

- Utilize an external hard drive.
- Use backup software provided by an external entity, such as cloud-based solutions.
- Manually copy files.

- Utilize a USB flash drive.
- Use optical disks, such as CDs or DVDs, to create a backup of your data.
- Utilize cloud storage, such: Google Drive, iCloud, Dropbox , Backb.
- Utilize online backup service
- Utilize Network-Attached Storage (NAS) device: It is a dedicated server that provides file-level storage and sharing for your home or small business network. It is operational and connected at all times, allowing you to access your data anytime and from anywhere.



Training cards

Pay attention!

Network-Attached Storage (NAS) device

It is a dedicated server that provides file-level storage and sharing for your home or small business network. It is operational and connected at all times, allowing you to access your data anytime and from anywhere.

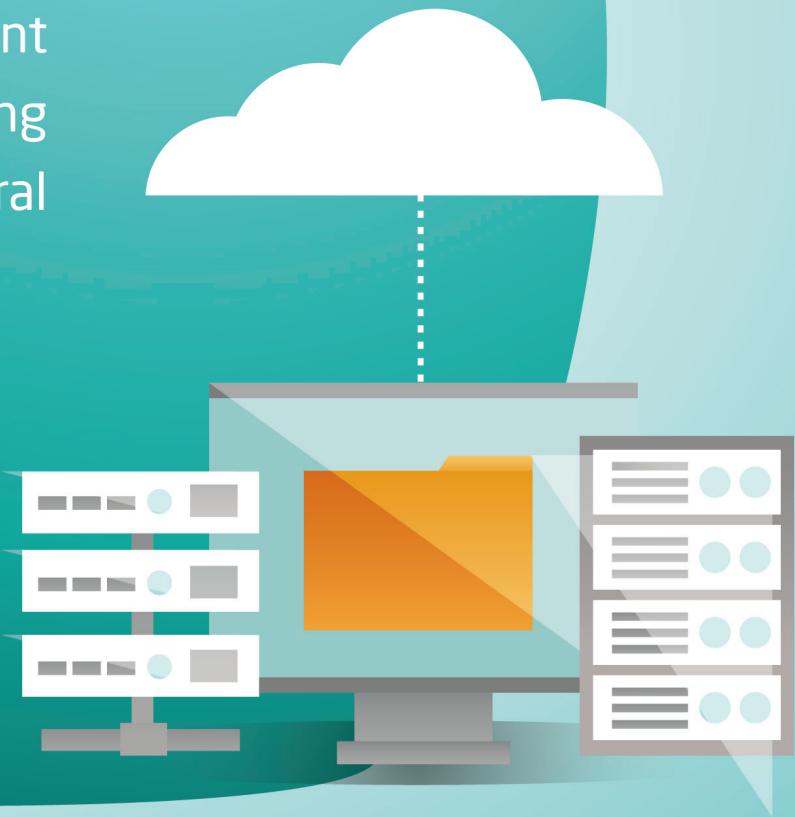


Pay attention!

Rule 1-2-3

It refers to creating 3 different copies of data, placing them on two different types of storage devices, and keeping one copy off-site. There are several ways to achieve this

- Utilize an external hard drive.
- Use backup software provided by an external entity, such as cloud-based solutions.
- Manually copy files.





Pay attention!

Definition of malware

It is a comprehensive term that describes any malicious software or code that damages systems. Deliberately seeking to invade computer devices, systems, networks, tablets, and mobile devices, it aims to damage or disable them, often by partially controlling device operations.

Pay attention!

Unauthorized Access (Illegal Access)

Unauthorized access involves gaining entry to computer resources without authorization. These resources may include a system, network, program, or data. Unauthorized access is typically perpetrated by hackers, but can also occur unintentionally. Individuals with legitimate access to the system may inadvertently encounter insecure files that were not intended for their perusal.



How to keep data secure

**Pay
attention!**

- 1 Use secure passwords, and change them from time to time.
- 2 Avoid utilizing the same password for multiple accounts.
- 3 Avoid writing down your passwords anywhere.
- 4 Multi-Factor Authentication
- 5 Exercise caution when sharing personal information
- 6 Limiting the sharing on social media platforms.
- 7 Close inactive online accounts.
- 8 Update your systems and software regularly
- 9 Be careful of free Wi-Fi services.
- 10 Utilize Antivirus programs.

Pay Attention!

Data theft

It involves the unlawful transfer or storage of personal, sensitive, or financial information. This can encompass passwords, source code, algorithms, processes, or proprietary technologies. It constitutes a grave breach of security and privacy.





**Pay
Attention!**

Ransomware

These are malicious programs designed to prevent users or enterprises from accessing files on their computer devices, demanding a ransom in exchange for restoring access to their files.

Information security

It refers to the means, tools, and procedures necessary to ensure the protection of information from internal and external threats. It is the discipline that studies how to provide confidential and secure protective measures for information and how to counteract attacks on it.

Pay Attention!





Network Security

It is part of the information security system that focuses on securing the use and integrity of the network, and thus the safety of data transfer and exchange processes. This field encompasses both hardware and software technologies. Network security targets and prevents a diverse range of threats from entering or spreading within your network.

**Pay
Attention!**

Sketches



**The most prominent digital threats in digital devices
(phones, computers, Tablets)**

01 **Data leakage.**

02 **Network spoofing.**

03 **Phishing Attacks.**

04 **Spyware.**

How ransomware operates

There are three essential stages that this process goes through

Infection
vectors and
dissemination.

Data encryption.

Ransom
demand.

How to protect against ransomware?

1 Awareness, training, and education on digital security and concepts of cybersecurity.

2 Regular data backup.

3 Patching vulnerabilities in systems that have not yet been patched.

4 User authentication mechanisms serves as a crucial countermeasure to protect against the exploitation of compromised or stolen passwords.

5 Reducing the attack surface through addressing

- Phishing messages.
- Remote access solutions.
- Unpatched vulnerabilities.
- Mobile malware.

How to mitigate active ransomware infections?

The infographic features a central teal circle with a white border and a drop shadow. Six rounded rectangular boxes are arranged around it, connected by thin lines. The boxes alternate in color: dark red, teal, dark red, teal, dark red, and dark red. Each box contains a specific mitigation strategy.

Isolating the device.

Ensure the availability of decryption tools.

Maintain the computer in an operational state.

Seek assistance from a specialized professional.

Creating a backup.

Reformat and Restore by installing the operating system to ensure that the malware is completely removed from the device.

How does data theft occur?

Data theft can be perpetrated using a diverse range of tools.

1 Social engineering.

2 Weak Passwords.

3 System vulnerabilities (security loopholes).

4 Internal threats by certain employees within an enterprise may possess access to customers' personal information, which could be exploited.

5 Human error

6 Installing software from untrusted sources.

7 Theft or loss of electronic devices.

8 Publicly Available Information.

Tips for detecting and preventing unauthorized access.

1

Establish a strong and complex password policy and change it from time to time.

Regular prompts and verifications concerning cybersecurity procedures through training.

2

3

Reducing the number of devices that can access sensitive data.

4

Securing all endpoints by installing antivirus software on each endpoint to remove and detect malware..

How can I determine if I am infected with malware?

- Your computer is performing poorly.
- The appearance of disruptive advertisements on the screen.
Your system crashes, manifesting as freezing or the infamous
- Blue Screen of Death (BSOD), the latter occurring on Windows systems.
- Mysterious loss of disk space.
- An unusual increase in internet activity for your system.
- Browser settings automatically change.
- The antivirus program stops working.
- Losing access to your files or the entire computer.



How to remove malware

1

Install and download good cybersecurity software to combat viruses and malware.

2

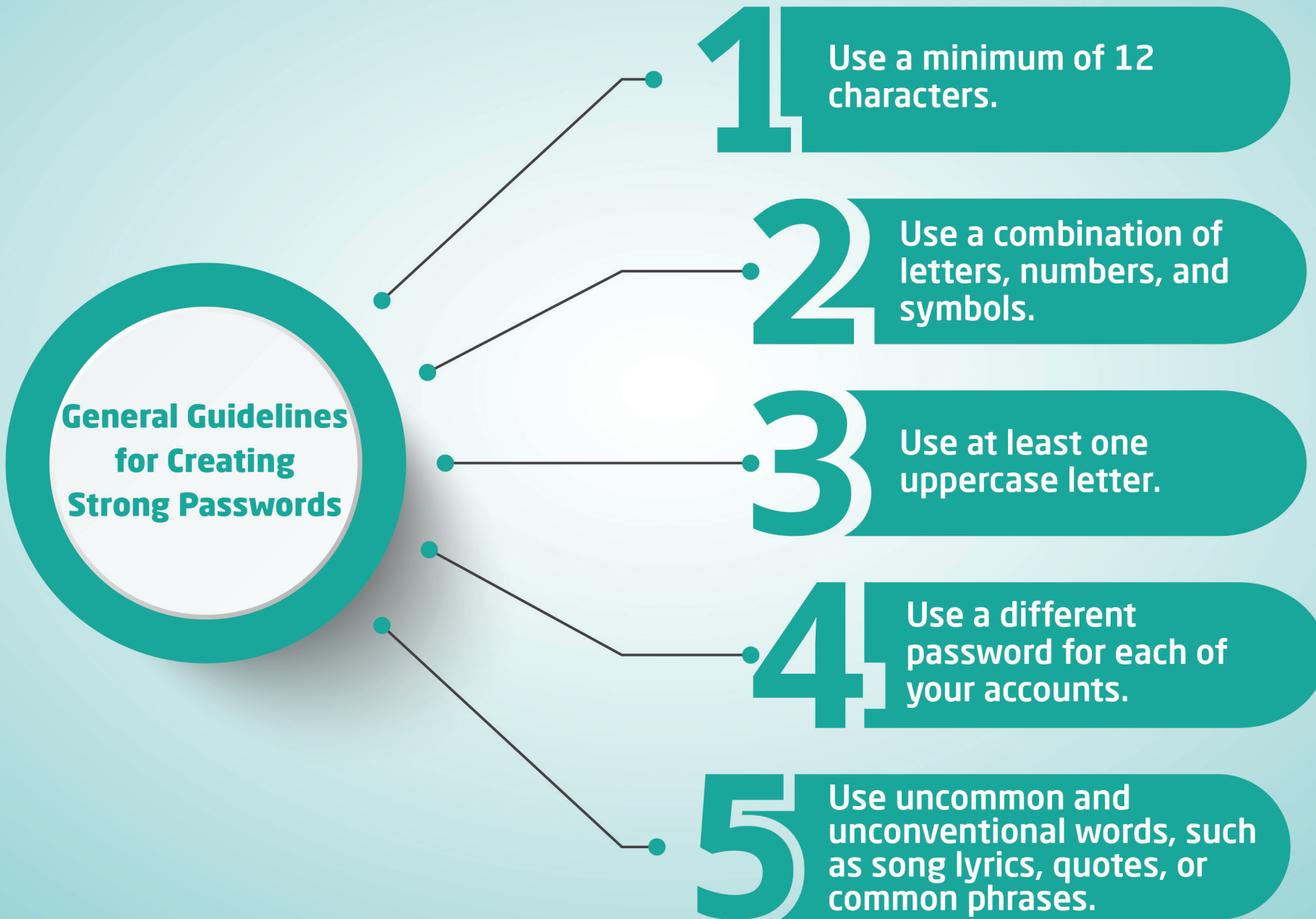
Run a scan using your new program.

3

Change all your passwords.

The Significance of Password Protection

It serves as the first line of defense against unauthorized access to accounts, devices, and files online. Strong passwords help secure data from malicious entities and malware. The stronger the password, the greater the protection of information.



**General Guidelines
for Creating
Strong Passwords**

The infographic features a central teal circle with a white border containing the title. Five teal lines radiate from the right side of the circle, each ending in a small teal dot. These lines connect to five teal rounded rectangular boxes, each containing a large white number and a corresponding guideline. The background is a light teal gradient.

1 Use a minimum of 12 characters.

2 Use a combination of letters, numbers, and symbols.

3 Use at least one uppercase letter.

4 Use a different password for each of your accounts.

5 Use uncommon and unconventional words, such as song lyrics, quotes, or common phrases.



CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency