Web bots

Presentation Slides

Training kit

High School

CyberEco

معاً لدعم السلامة الرقمية

Together to support digital safety

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

Intellectual Property rights

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

November, 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:

لوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa
00974 404 663 78
00974 404 663 62

Time Table for the Lecture

Content	Allocated Time
General introduction	5 minutes
The theoretical aspect	25 minutes
Educational Videos	25 minutes
Short break	20 minutes
Training games	25 minutes
Dialogue and discussion with students	15 minutes
Graduation project	2 minutes
Total training time	2 hours

Chapter One
The concept of web bots and their types

The concept of web bots

Bots

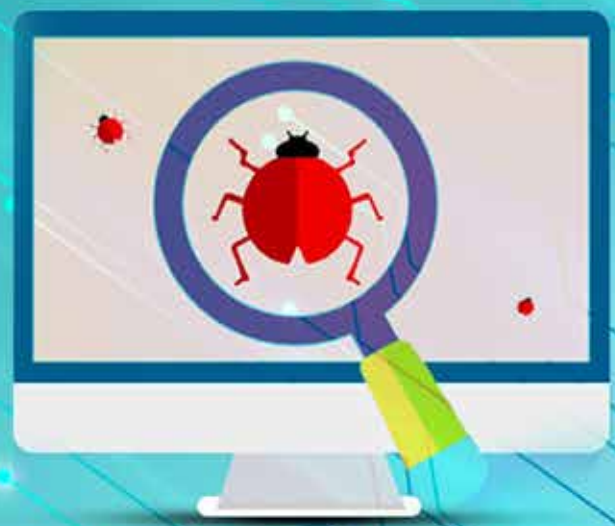
It is a program that performs automated, repetitive, and predetermined tasks. Bots typically mimic or replace human user behavior, but they operate much faster than humans. Bots can perform useful functions, such as customer service or indexing search engines. However, they can also come in the form of malicious programs that are used to take full control of a computer.

Web bots are also referred to by other names such as: spiders, crawlers, or web bots.

Definition of malicious bots

They are internet-connected devices, each of which runs one or more bots, often without the knowledge of the device owners, since each device has its own IP address, botnet traffic comes from multiple IP addresses, making it difficult to identify the source of malicious bot traffic and block it.

Botnets can also evolve themselves by using devices to send spam emails, which can infect more devices.



The mission of malicious bots

Malicious bot programs and web bots can be programmed to hack into user accounts, scan the internet for contact information, send spam, or perform other malicious activities. Attackers distribute malicious bots across a botnet to carry out these attacks and conceal the source of the attack traffic.

Types of web bots

Bots

They are software applications designed to automate specific tasks and interact with users, often simulating human conversation in the case of chatbots. They are programmed to follow predefined rules or utilize artificial intelligence (AI) algorithms to process natural language and provide responses.

The importance of bots

Efficiency

bots can handle repetitive and routine tasks much faster than humans, increasing overall efficiency and productivity.

Personalization

Advanced bots with artificial intelligence capabilities can learn from user interactions, providing personalized experiences over time.

Availability

Bots can work 24/7, providing immediate assistance to users without the need for human intervention.

Low cost

By performing tasks, bots can help reduce labor costs and improve resource allocation.

Scalability

Bots can handle multiple interactions at the same time, making them ideal for dealing with large volumes of inquiries or operations.

Bots are generally divided into two main types

01 Chatbots:

It is a bot designed to participate in conversations with users, typically through text or voice interfaces.

02 Task automation bots:

This type of bots concentrates on automating repetitive tasks, data processing, and other routine activities that could consume a significant amount of time for humans.

What are good bots?

Good bots are designed to perform legitimate activities, in contrast to malicious bots and they come in various types, including:

01

Search engine bots

Also known as web crawling programs.

02

Backlink checker bots

Backlinks are considered crucial for improving Search Engine Optimization (SEO), aiding in the discovery of backlinks to a specific web page and analyzing its progress and quality.

03

Social media bots

It is designed to automate tasks on social media platforms.

04

Chatbots

Its primary objective is to provide customer assistance around the clock, seven days a week.

05

Game bots

Designed specifically to perform activities related to gaming, such as simulating real players in games.

06

E-commerce bots

Provide product recommen-dations and assists in purchasing products.

Malicious bots

These are bots designed to engage in various malicious activities. They exploit vulnerabilities to gain unauthorized access to user accounts. Malicious bots can also target specific enterprises to tarnish their reputation on social media by spreading fake news or sending spam emails to everyone they know.

Malicious bots types

01 DDoS bots

These bots are designed to launch Distributed Denial of Service (DDoS) attacks on websites, networks, or servers.

02 Spam Bots

Spam bots can send unwanted messages to targets, such as launching phishing attacks or posting negative comments on social media to tarnish the image of a specific brand or company, as well as promoting illegal products or services.

Malicious bots types

03 Account takeover (ATO) bots

Also known as ‘credential stuffing bots,’ they can access user accounts by using stolen usernames and passwords.

04 Malware distribution bots

These bots have the capability to distribute malicious software, such as ransomware, viruses, trojans, worms, and others, by exploiting vulnerabilities in the targeted systems and spreading the malicious programs.

Malicious bots types

05 Exploitative bots

This bot is designed to purchase fast-moving products or services in large quantities.

06 Clickbots

It deceives advertisers through artificial user clicks, manipulating search engine rankings.

Risks of malicious bots

Manipulation of content

As it leads to the spread of misinformation or the creation of a distort-ed perception in the public opinion.

Violations of data privacy

Bots may exploit weaknesses in systems to gain unauthorized access to sensitive user data, leading to privacy violations and identity theft.

DDoS Attacks

Botnets, which are networks of compromised computer devices controlled by a single entity, are used to launch attacks against servers and disrupt services.

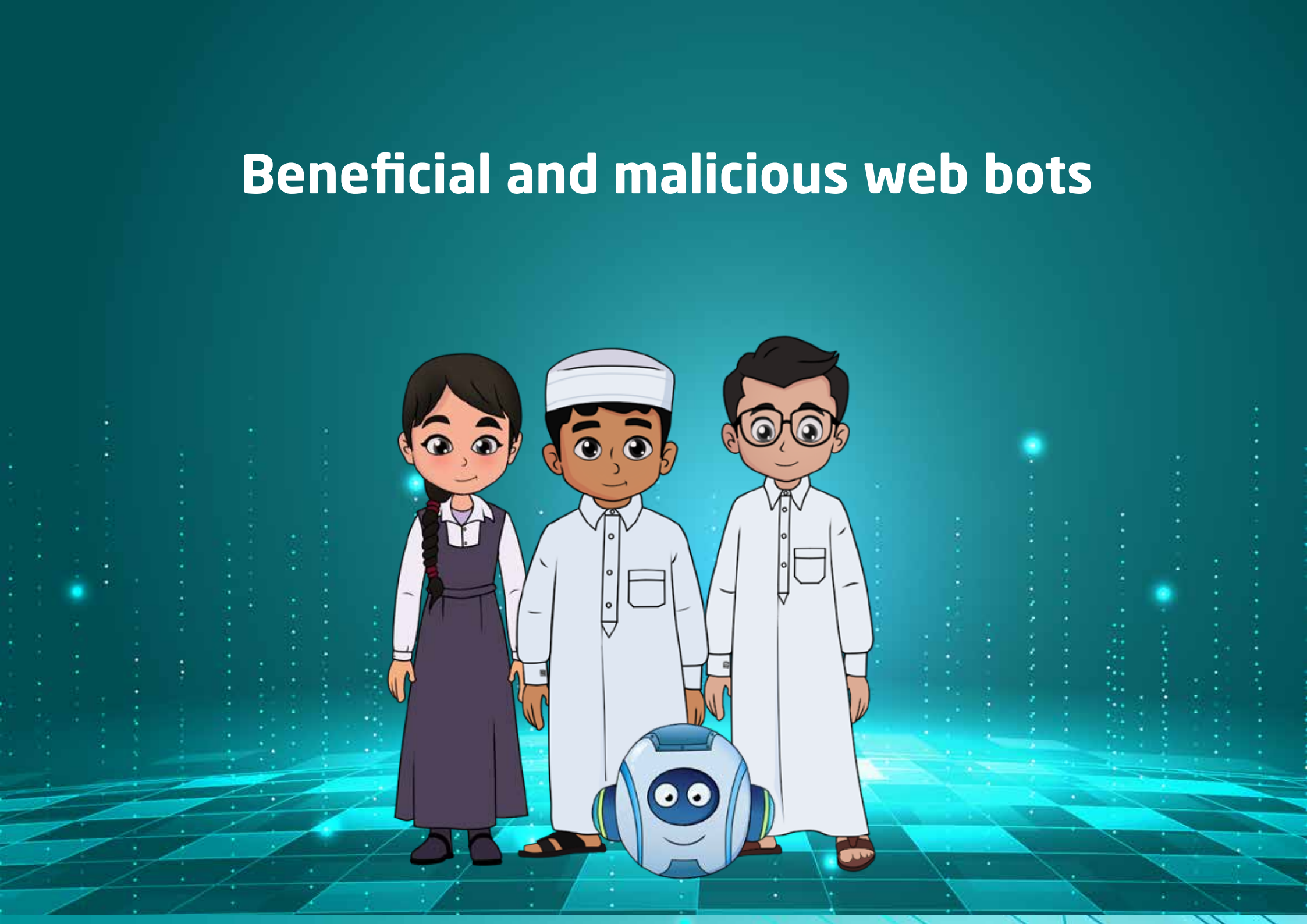
Diminution of trust

Malicious bot attacks lead to a decrease in user trust in online platforms and companies.

Fraud and theft

Malicious bots can be utilised to execute fraudulent activities such as account takeover, theft of personal identification information or the spread of misleading information.

Beneficial and malicious web bots



Beneficial bots

These bots play a fundamental role in the web ecosystem, serving as automated programs designed to perform specific tasks that benefit users and website owners. They serve legitimate purposes such as web content indexing, enhancing search engine visibility, data collection for directories, improving user experience.

Beneficial bots types

01 Spiders (web crawling programs)

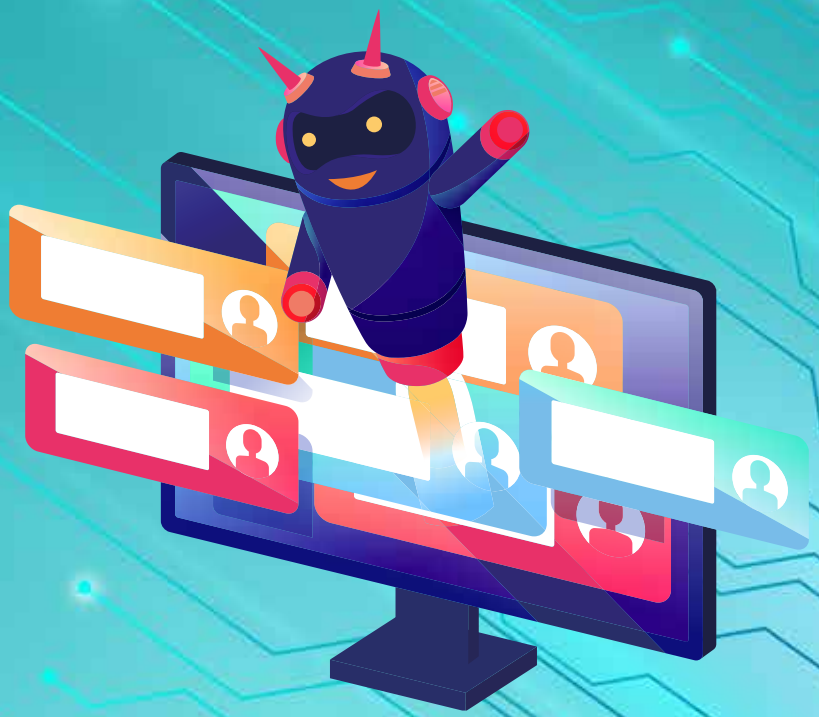
These bots crawl websites, gather information, and index it in the search engine's database.

02 Data collectors

These are bots designed to gather information from various sources and create comprehensive directories or content lists. These bots collect and update data to provide users with up-to-date information about websites, companies, products, or services.

What is a bot attack?

It is a type of cyber attack that utilizes automated scripts to disrupt a website, steal data, perform fraudulent purchase transactions, or execute other harmful actions. These attacks can be deployed against various targets, such as websites, servers, and applications, and their purposes vary, but they often involve the theft of sensitive information or causing damage to the target's infrastructure.



Malicious bots types

01 Credential stuffing

It is a cyber attack in which compromised credentials obtained from a data breach are utilized.

02 web/content scraping

It occurs when bots download content from a website to use it in future attacks. A data scraping bot sends a series of requests to a website, copies the information, and saves it, all within a matter of seconds.

Types of web/content scraping

Communication scraping

Price scraping

This occurs when a company downloads all pricing information from a competitor's website, enabling it to adjust its own prices accordingly.

Malicious bots types

01 DDoS attack

A Distributed denial of service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network.

02 Brute-force attack

The brute-force attack is a trial-and-error method used to decrypt sensitive data, and the most common applications of brute-force attacks are password cracking and breaking encryption keys.

Preventive measures against brute force attacks

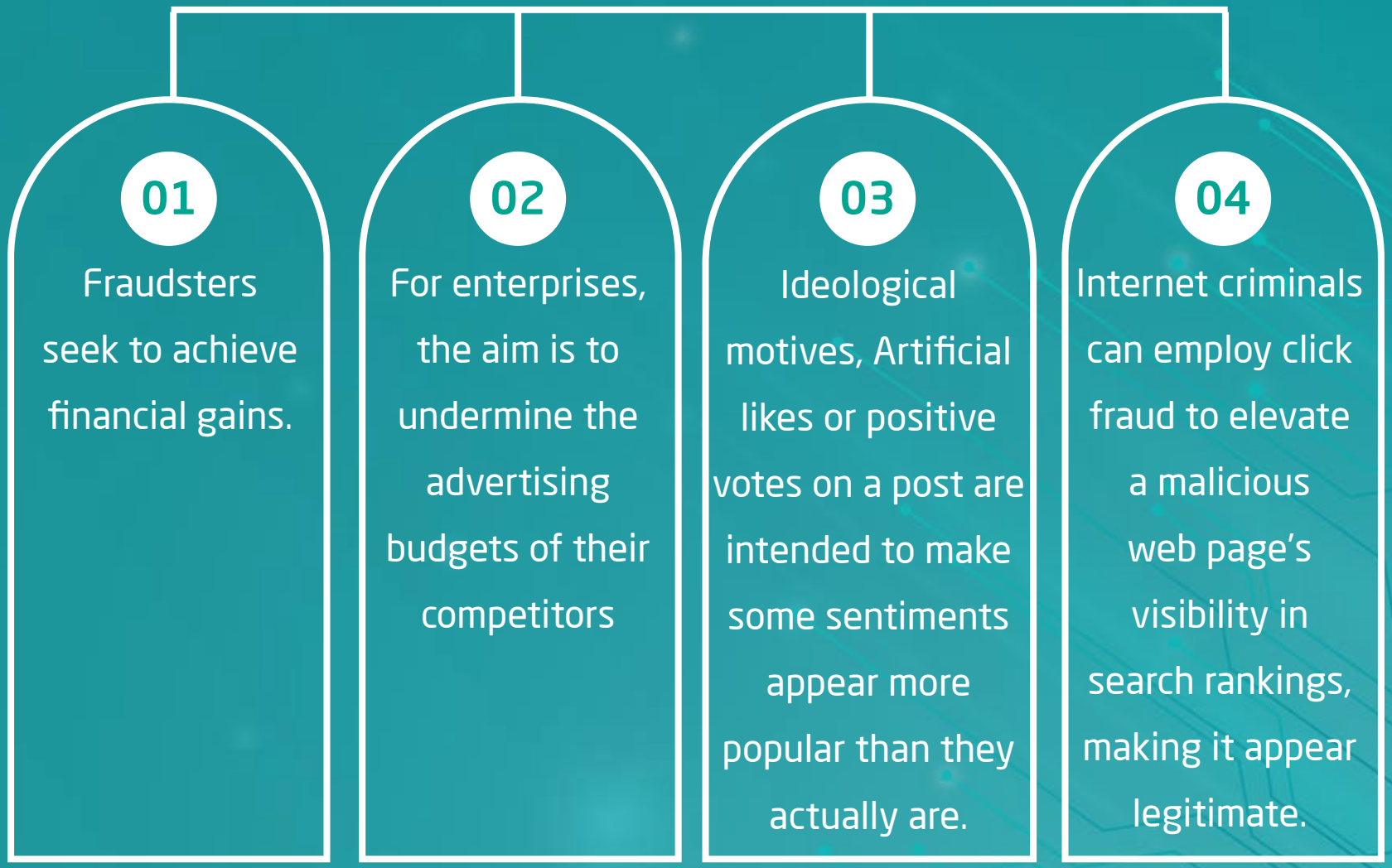
- Choosing longer and more complex passwords.
- Enabling two-factor authentication and using unique passwords for each service.
- Avoid entering passwords or personal information such as credit card numbers or banking details into any web service that does not secure their data with strong encryption keys.

Malicious bots types

03 Click Fraud

Click fraud occurs when a person or a bot pretends to be a legitimate visitor to a web page and clicks on an advertisement, button, or any other type of branching link (internal links). The purpose of click fraud is to deceive the core system or service into believing that genuine users are interacting with a web page, advertisement, or application.

Motivations for Click Fraud



Common Types of Click Fraud

- Advertising fraud.
- Internet fraud.
- A financial attack on the company that pays for advertisements.
- Manipulating search engine rankings through increased click-through rates with the aim of appearing artificially elevated.

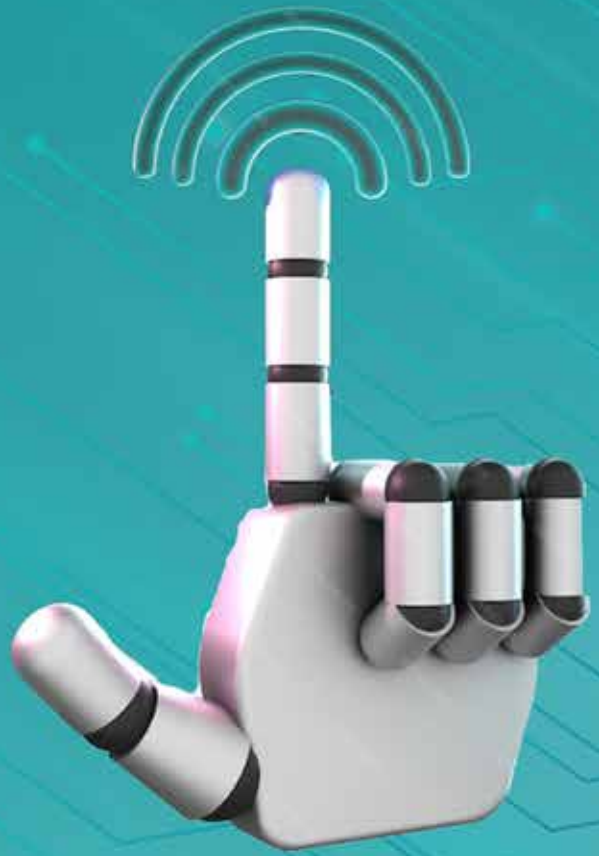
What is a click bot?

It is a bot programmed to carry out click fraud. The simplest click bots merely access a web page and click on the specified link, Well-programmed click bots are designed to mimic actions that a real user might take, such as mouse movements, random pauses before taking an action.

Does click fraud only occur from bots?

It can also be executed by human workers with low wages.The term ‘click farm’ is used to describe a group of these workers, and click farms are often operated in regions where wages are relatively low, as is the case in developing countries.

Workers in a click farm navigate to specific web pages and click on designated links to artificially inflate click rates or overall traffic statistics for those pages. They can also be active on social networks, ‘liking’ posts or specific pages to boost their visibility.



Chapter Two: The operation mechanism of web bots and their benefits

How do web bots operate?

The structure of a bot typically includes the following:

01

Application logic

It is the executable and automatically readable code written by the bot developer and executed by the computer.

02

Database

It is the dataset from which the bot derives information about the actions to be taken.

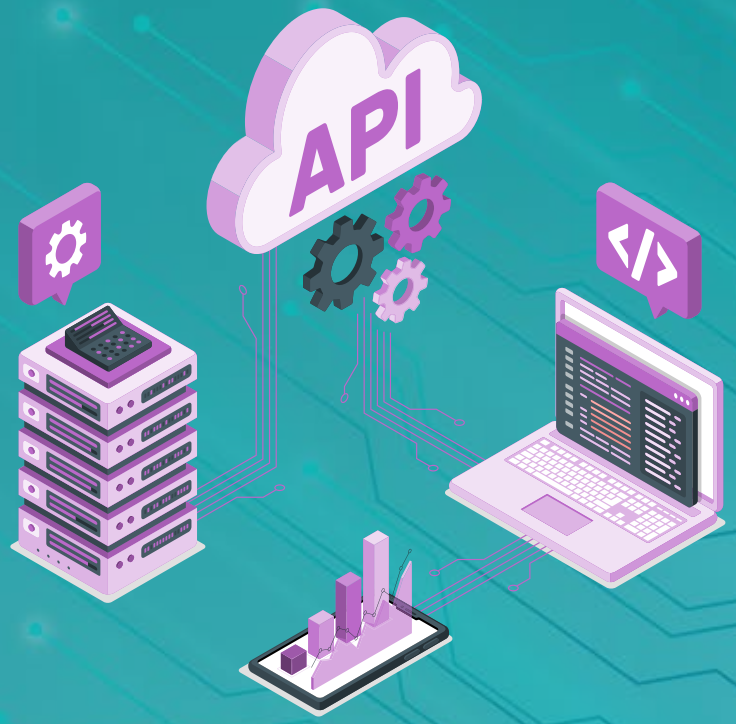
03

API Integrations

Application programming interfaces enable the bot to utilize external functions without the developer having to write them.

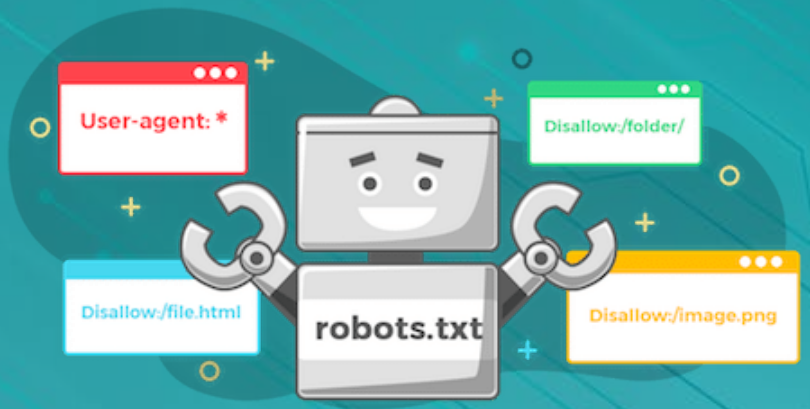
Application programming interface (API)

It is a means to integrate complex software functions created by someone else. For example, a chatbot can use the weather application to provide detailed information about the weather if users request it. In this way, the chatbot does not need to track the weather itself; it simply calls the 'Weather' application programming interface.



What is the robots.txt file?

robots.txt is a file located on a web server that outlines rules for bot access to the properties on that server. Anyone programming a bot should ensure that their bot checks the robots.txt file of the website before accessing it. Naturally, malicious bots do not adhere to this system, hence the need for bot management.



Bot management

Bot management refers to blocking the traffic of unwanted or malicious bots on the Internet while allowing access to beneficial bots to web properties. Bot management achieves this by detecting bot activity, distinguishing between desired and undesired bot behavior, and identifying sources of unwanted activity.

The importance of bot management

01

In the case of leaving bot traffic undefined, it can cause significant issues for web properties.

02

The very substantial traffic of bots can lead to an increased load on web servers, causing service slowdowns or denials for legitimate users.

Bot Manager

It is a software product that manages bots, where bot managers can block some bots and allow others to pass, instead of simply blocking all non-human traffic; because if all bot programs like Google bot are blocked and cannot index a page, that page will not appear in Google search results; resulting in a decrease in the number of visits to the website.

Objectives of a good bot manager

- Distinguishing between bots and human visitors.
- Evaluating the reputation of the bot.
- Determining the original IP addresses of the bot.
- Analyzing the behavior of the bot.
- Adding beneficial bot programs to the allowed lists.
- Limiting the excessive use of bots for service.
- Denying malicious bots access to specific content.
- Providing alternative content for the bots.

What are the benefits of web bots?

Task automation

Bots excel in automating repetitive tasks, saving time and effort for both enterprises and individuals.

Enhanced efficiency

The Bots operate around the clock without interruption, ensuring continuous service availability.

Scalability

Bots can handle a large number of simultaneous interactions, making them highly scalable solutions.

Data Analysis

Bots capable of task automation can process vast amounts of data quickly and accurately. This facilitates the acquisition of insights and making data-driven decisions.

Enhanced user experience

In e-commerce, chatbots can provide personalized assistance, guide users through processes, and suggest products or services based on their preferences.

Securing devices and files from malicious bots

Indications of devices and files being affected by the botnet

- Decreased processing speeds.
- Frequent application crashes
- Slow internet speed.
- Increase in the number of unauthorized social media posts and unauthorized email messages.
- Existence of unfamiliar files and applications that you have not downloaded or installed.

What should you do if your device is infected with botnet malware?

- Disconnect your device from any WiFi network.
- Identify malware using antivirus software, or you can manually search for any suspicious files.
- Remove malware automatically or manually, with the automatic method being preferable as it ensures the complete removal of infected files from your device.
- Reset your device and reinstall your operating system.
- Report the infection of the bots to the relevant authority.

How to prevent bot Attacks

- Avoid clicking on suspicious links.
- Avoid downloading any email attachments from unfamiliar senders.
- Do not download software or programs from unverified sources. such as free programs from the internet.
- Activate the firewall on your device.
- Change the default password settings on your smart devices.
- Keep your internet of things devices on a separate Wi-Fi network.
- Set up a guest network on your WiFi router.
- Regularly update the operating system and other software.
- Install antivirus software.

Examples of bot attacks

EarthLink Spammer 2000
EarthLink Spammer

It is the first recorded instance of a bot attack, where an unwanted botnet was utilized to send email messages to unsuspecting users in the hope of obtaining their financial credential data.

Mariposa 2008

It is a Spanish botnet aimed at stealing credit card numbers and infected nearly 10 million devices at its peak. And this makes it one of the largest botnet ever discovered. The botnet was dismantled by Spanish law enforcement authorities who managed to uncover the criminals behind it.

Necurs Botnet 2012 Necurs

It is a massive botnet that infected nearly nine million computers worldwide. It was used to distribute spam and dangerous malware, including the infamous banking Trojan GameOver Zeus. However, the Necurs botnet was successfully disabled by Microsoft and its partner agencies in 2020.

Mirai Botnet 2016

Mirai is one of the most infamous bot attacks, specifically targeting smart devices in the internet of things. The original creators of Mirai were apprehended, but its source code still exists and has been utilized to launch large-scale DDoS attacks over the years.

Glupteba Botnet 2019

It is a new type of bot that primarily targets Windows devices to mine cryptocurrencies and steal user credentials. Google disabled Glupteba in 2021, but it has resurfaced since then, indicating the resilience provided by the blockchain-based architecture.


First:
In-Class Exercises

Exercise I

Complete the following sentences:

1. Internet bots are known as ..... web or ..... net.

2. Web bots undertake ..... automated online, forming part of ..... handling ..... and intricate tasks .....

3. Web bots carry out both simple and complex tasks repetitively at a rate ..... than what ..... can achieve.

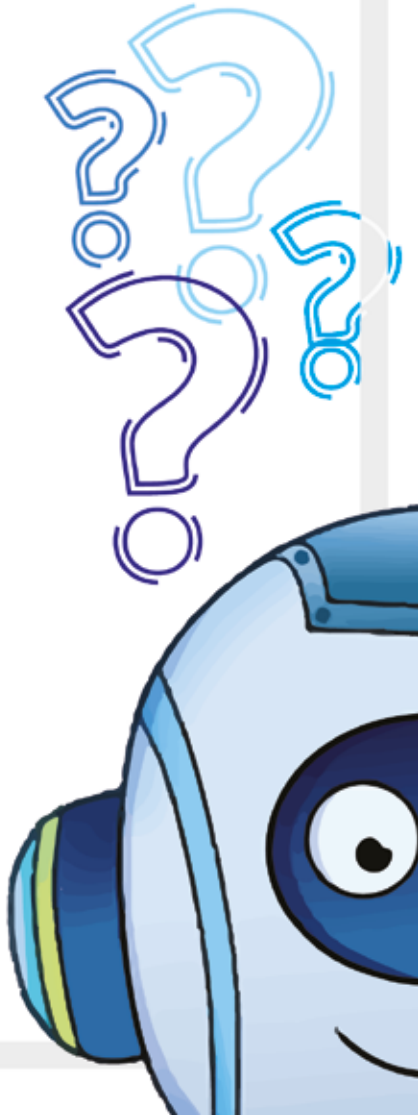
4. The primary mission of web bots is ..... Web pages, as they are responsible for extracting and .....information from web servers ..... and ..... swiftly than .....

5. Each server possesses file ..... for indexing, encompassing all the regulations dictating the behavior of ..... on that server.

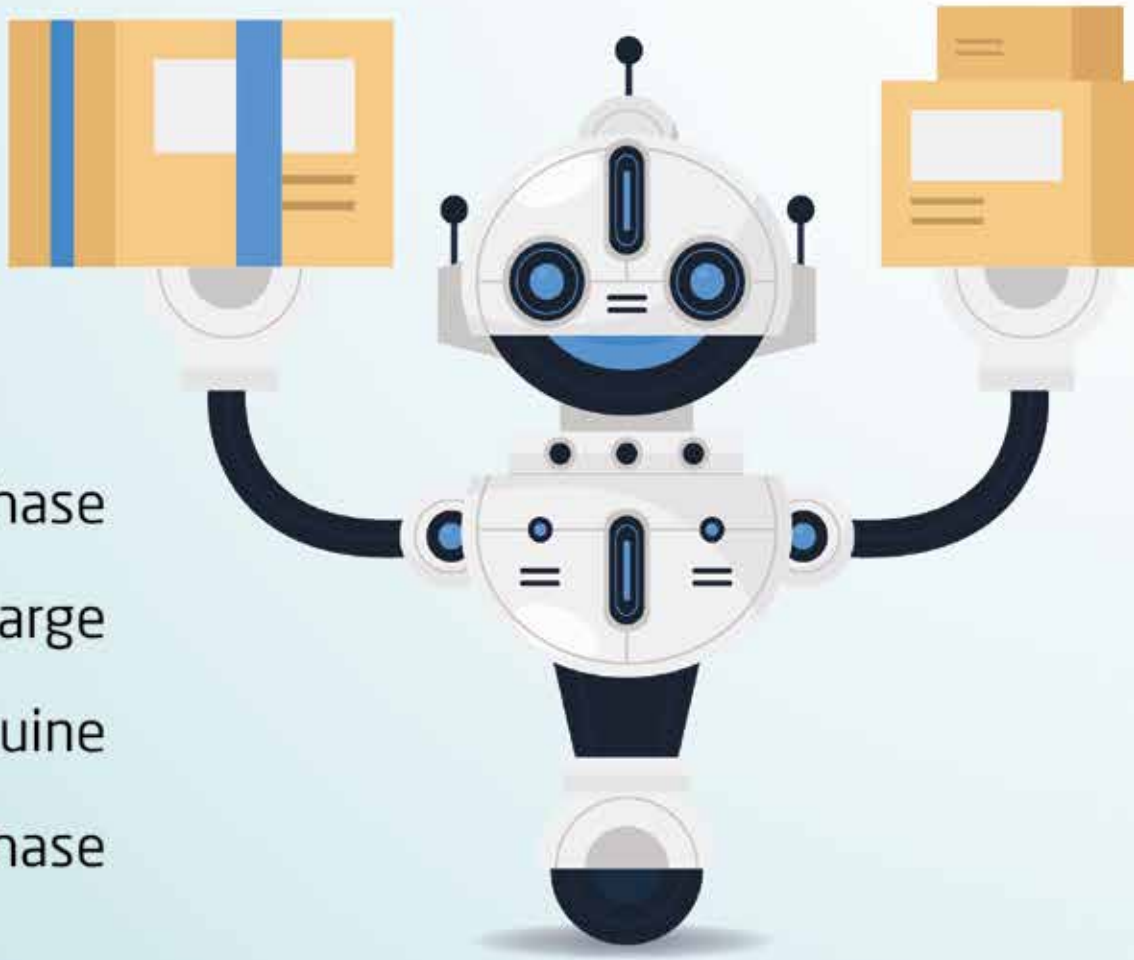
6. Social media platforms also depend on social ....., which are ..... responsible for executing ..... operations to create a service or ..... among social media users.

7. Social bots also monitor chat ..... and ..... designed for interacting with ..... users.

8. ..... on media platforms are designed to emulate ..... to collect patterns .....similar to user pattern.



Did you know that...?



Exploitative bots are designed to purchase fast-moving products or services in large quantities, making it difficult for genuine customers to complete legitimate purchase transactions.

Pay attention!

Malicious bots

They are internet-connected devices, each of which runs one or more bots, often without the knowledge of the device owners.

Since each device has its own IP address, botnet traffic comes from multiple IP addresses, making it difficult to identify the source of malicious bot traffic and block it.

Exercise 2:

Choose the correct word or phrase from the words or phrases provided within parentheses:

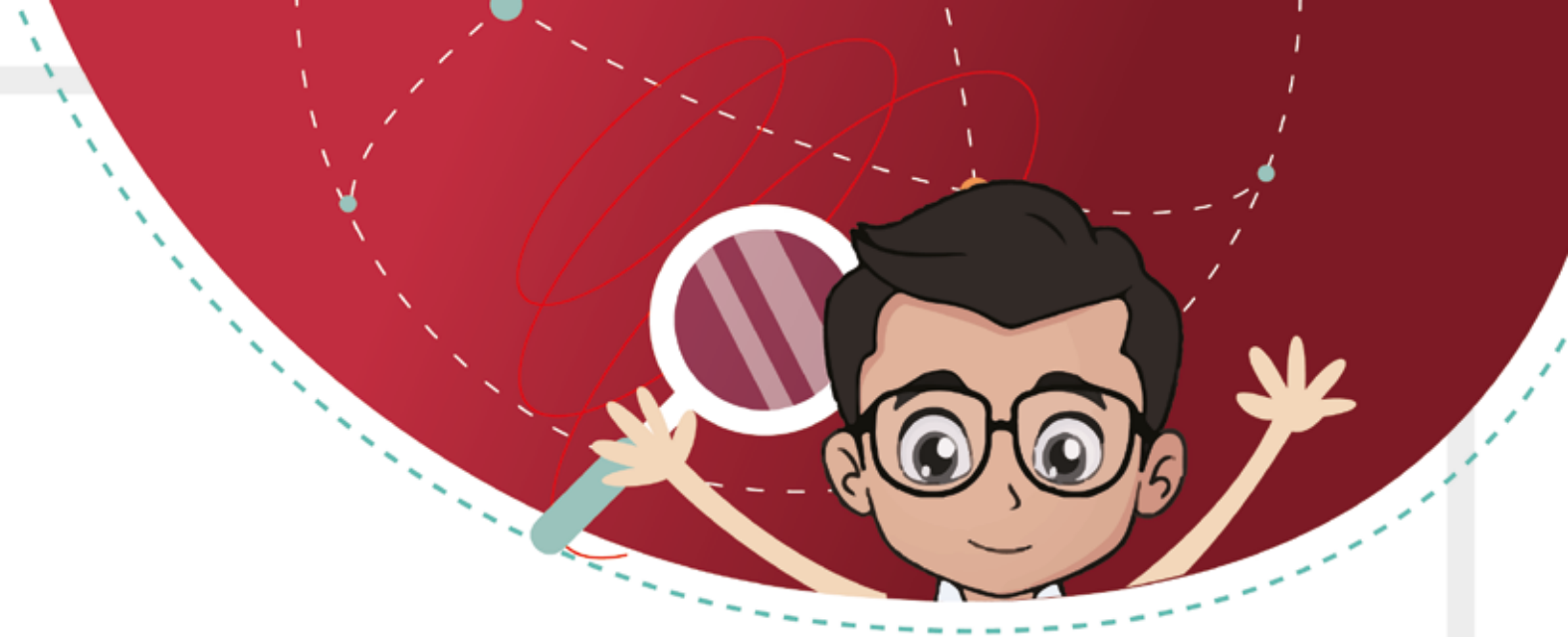
1. A bot is an abbreviation of the word robot, and it is a program that performs tasks (automatically ☑ manually ☐).

2. Web bots perform tasks (repeatedly ☐ once only ☐).

3. Web bots are considered to be (as fast as humans ☐ faster than humans ☐).

4. Web bots can perform tasks that are (useful ☐ unimportant ☐).

5. The most important tasks performed by bots are (customer service and search engine indexing ☐ securing personal accounts for users ☐).



6. Web bots can be malware if they (lose control ☐ take full control of the user's computer ☐).

7. Computer bots are considered to be (digital tools ☐ security programs ☐).

8. Sometimes, bots are misused and exploited to attack (websites ☐ personal accounts ☐).

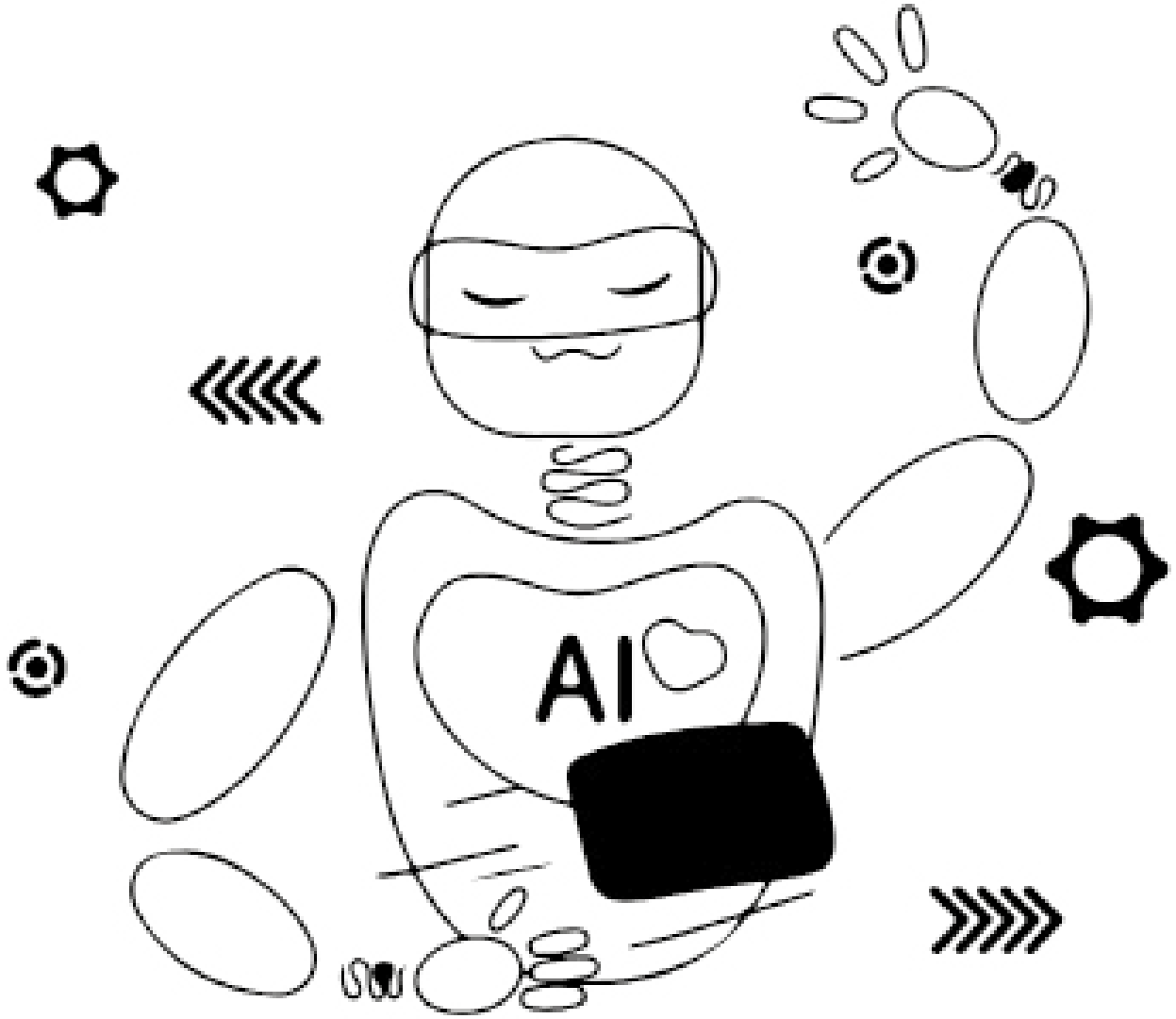
9. Web bots can (mimic ☐ control ☐) human behavior.

10. Malicious bots can (promote ☐ disrupt ☐) businesses and attack websites.

Pay attention!

Downloads

One of the most common ways that bots infect a user's computer, phone and table. This is done by receiving malware in download format through social media or email messages that advise you to click on a link. The link is often in the form of an image or video, and contains either viruses or other malware.


AI

Exercise 3:

Identify the true ✓ and false ✗ statements in the following sentences:

Orientation

Read the sentences in the table carefully, and think if the information is true or false, and if you find it correct, write next to it (true), and if you find it wrong, write next to it (false), ask for the help of the trainer if you need it

1	Web bots are programs that operate only after obtaining user permission.	✓
2	Bots perform tasks one at a time.	
3	Web bots are considered to be highly efficient and much faster than human performance.	
4	Web bots only perform harmful tasks.	
5	Bots can perform tasks such as customer service and website indexing.	

6. Web bots are incapable of engaging in any harmful activities.

7. Occasionally, web bots target only certain small websites.

8. Web bots are exclusively used by companies.

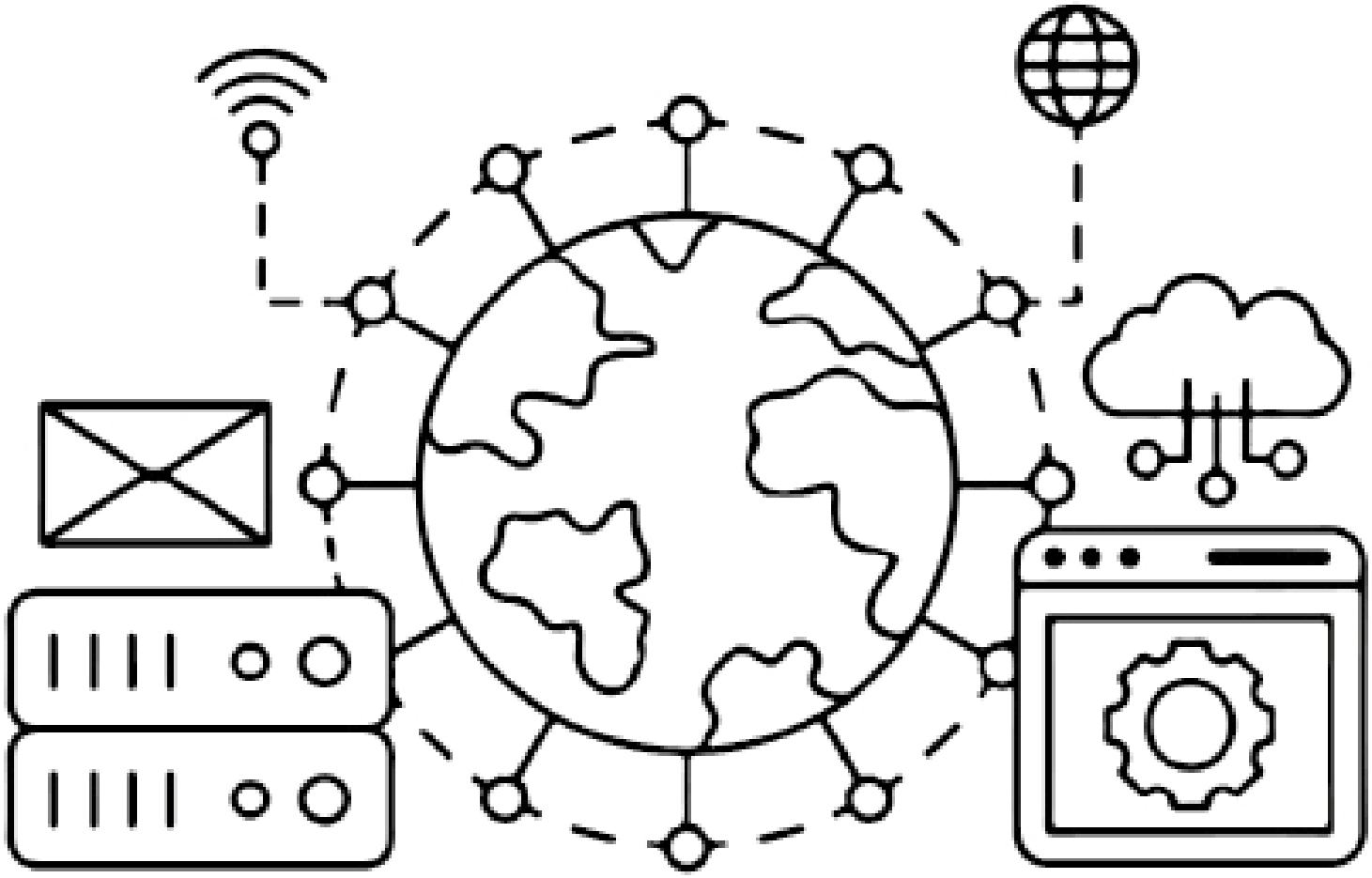
9. Web bots contribute to only 1% of the daily operations of the internet.

10. Web bots are considered the primary drivers of search engine optimization.

Pay attention!

Chatbots

It is a bot designed to participate in conversations with users, typically through text or voice interfaces, using technologies such as Natural Language Processing (NLP) and Artificial Intelligence (AI) to understand user queries and provide relevant responses.



Exercise 4:

Assign the appropriate bot type to each of the following sentences:

Instruction

Read the phrases in the table carefully, and consider what type of bot each phrase refers to. Write the type of bot in the corresponding column. An example is provided below.

1	These are bots that simulate human conversations by responding with predefined sentences.	Chatbots
2	These are bots that operate on social media platforms and are used to create automated messages, focus on specific ideas, and monitor fake accounts.	
3	These are bots that assist you in finding the best prices for products and monitor usage patterns to suggest specific products that may suit you.	
4	These are bots capable of examining the content available on the internet and assisting in handling user queries and responding to their inquiries.	
5	These are bots that read data from websites and can store it for use or reuse, often assisting in preventing information theft and securing copyright and publishing rights.	

6	These are bots specialized in gathering information for users by automatically visiting websites to retrieve information and respond to specific questions.	
7	These are bots used to monitor the status of websites or systems and assist in providing real-time information.	
8	These are bots used to complete transactions on behalf of human users, allowing users to conduct transactions within the context of the	
9	These are bots used to automatically download programs or applications from specialized app stores.	
10	These bots operate automatically to purchase tickets for popular events with the intention of reselling them for profit, constituting an illegitimate activity in many countries around the world.	

Pay attention!

Task automation bots

It is a type of bots concentrates on automating repetitive tasks, data processing, and other routine activities that could consume a significant amount of time for humans.

Did you know that...?

Credential stuffing bots can gain access to user accounts by launching attacks that involve utilizing stolen usernames and passwords or infiltrating user accounts.

Exercise 5:

Classify the following bots as malicious or beneficial:

• Spam.	**Malicious bots.**
• Spider bots or web crawlers.	
• Chatting to deceive people.	
• File-sharing bots.	
• Ticket bots.	
• Monitoring bots.	
• Transaction bots,	
• Entering credentials.	
• DDoS attacks.	
• Download bots.	
• Web scraping crawling bots.	

Exercise 5:

Classify the following bots as malicious or beneficial:

• Automated conversation response bot.	
• Denial of Inventory Attacks.	
• Information Gatherers.	
• Vulnerability scanners.	
• Store bots.	
• Click Fraud bots.	
• Activity monitoring.	
• Social bots.	

Pay attention!

Search engine bots

It is a type of beneficial bots, also known as web crawlers, these bots are used by popular search engines like Google, Yahoo, and Bing to crawl the internet and find the information needed by users.

Exercise 6:

The following sentences are incorrect... Identify the errors and then correct them:

Instruction:

Read the sentences below carefully, identify the error in each sentence, and correct it. An example is provided in the table.

Web bots cannot communicate with each other.

web bots can communicate with each other.

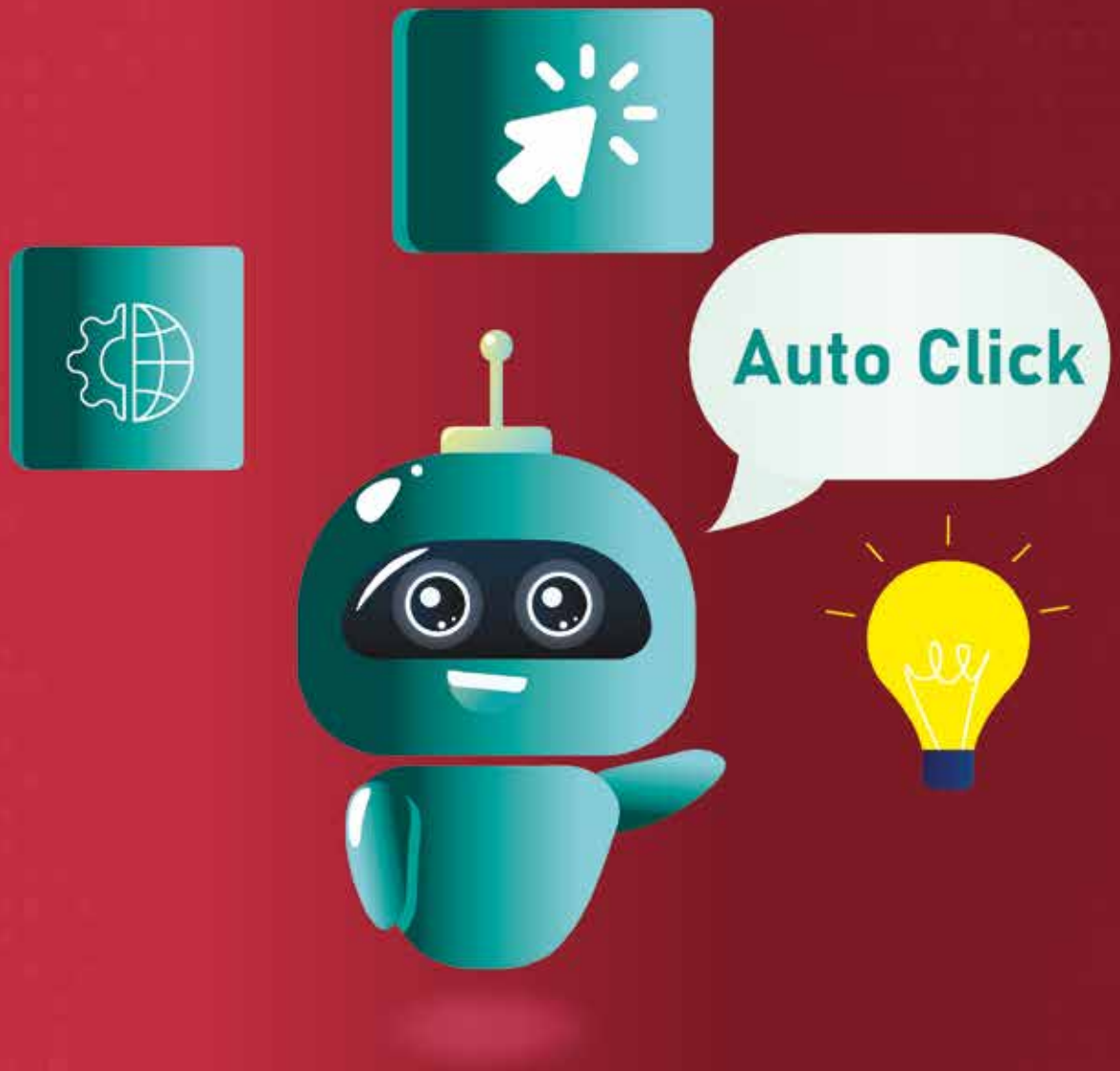
Algorithms are a non-essential part of bots and do not have significant importance.

Chatbots operate automatically without specific pre-defined commands.

Bots cannot learn from humans.

Bots do not use artificial intelligence technologies.


Second:
Non- Classroom
exercises



Pay attention!

Clickbots

Clickbots can automatically click on links present on websites, resulting in the generation of a substantial volume of traffic. Consequently, this deceives advertisers through artificial user clicks, misleading search engine rankings.

Exercise 1:

Classify the following sentences as either disadvantages or advantages of bots:

Instruction

Carefully read the sentences below, and determine whether they express advantages or disadvantages of bots.
An example is provided below.

1. Faster than humans, especially in repetitive and patterned tasks.	**Beneficial**
2. Saves time for customers and clients.	
3. Reduces labour costs for companies.	
4. Its programming may be malicious.	
5. They are not capable of performing all tasks, and ignorance of them may lead to risks.	
6. Available 24/7.	
7. It can be used in spam.	
8. Enables companies to reach a wider audience through messaging applications.	
9. Customizable.	
10. It cannot function without human management intervention on occasion.	
11. Multipurpose.	
12. It can enhance the user experience.	

Pay attention!

Data collectors

These are bots designed to gather information from various sources and create comprehensive directories or content lists. These bots collect and update data to provide users with up-to-date information about websites, companies, products, or services.

Exercise 2:

Arrange the following steps in the event that your computer is infected with a bot virus:

Instruction

Read the sentences below carefully, and identify the sentence that indicates the first step in the event of infection with a bot virus, and the second, and the third, and so on until the end of the sentences.

1	Transfer all important or personal data to another device or an external hard drive.	
2	Secure the computer using various security tools or seek the assistance of a professional to do so.	
3	Disconnect the computer from the network as quickly as possible to prevent data and information theft.	
4	Restore your device to factory settings, and this will resolve the issue, though unfortunately, all files on your device will be deleted.	

Exercise 3:

Mark True or False in front of the following phrases, correcting them if they are false:

1. You cannot, under any circumstances, fully protect your device 2.

2. Installing anti-malware software helps protect your device from bot attacks.

3. Neglecting software updates has no impact whatsoever.

4. Using strong passwords can help to prevent many security problems.

5 You can click on links on the internet without fear.

6 There are no unreliable websites or ads.

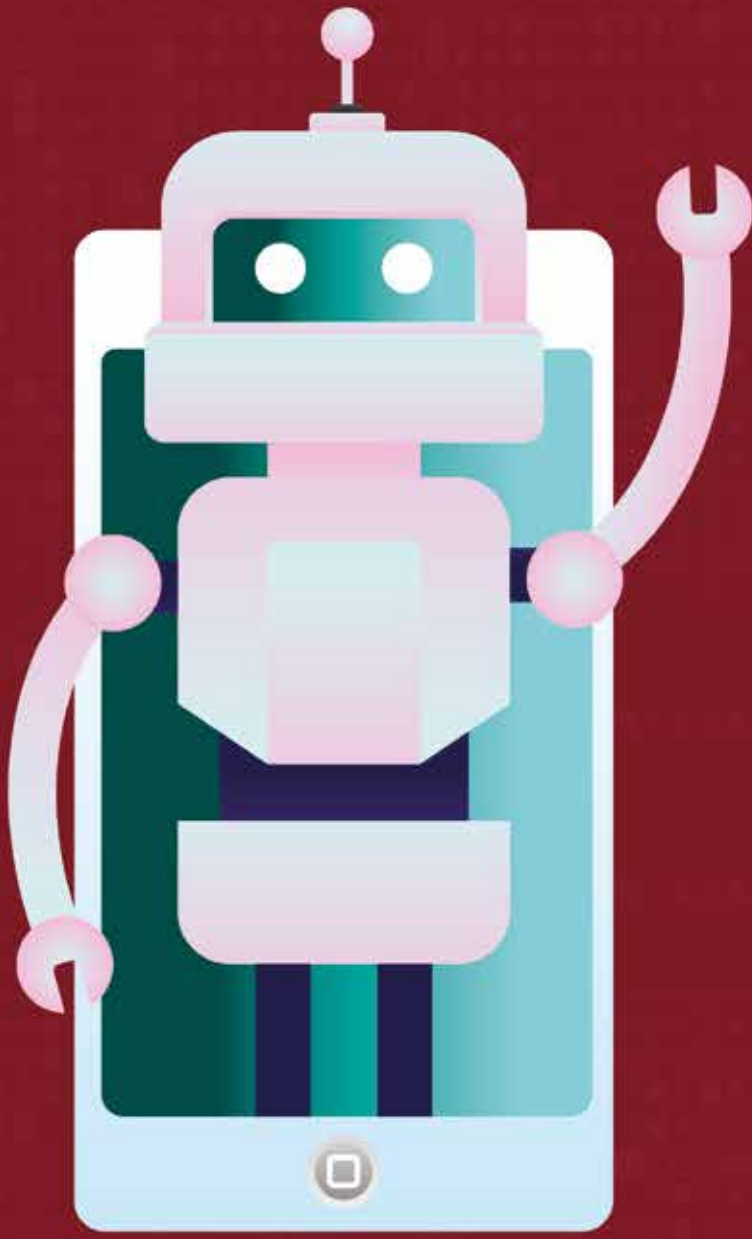
7 It is important to install a firewall to help block malicious attacks.

8 Using a bot manager does not affect malicious bots.

Pay attention!

Bot Attack

It is a type of cyber-attack that employs automated scripts to disrupt a website, steal data, carry out fraudulent purchase transactions, or perform other malicious activities. These attacks can be deployed against various targets, such as websites, servers, and applications. The purpose of these attacks varies, but they often involve stealing sensitive information or causing damage to the target's infrastructure or damage to reputation.



Exercise 4:

Extract the following words from the table.:

Instruction

Read the words below carefully and search the table for consecutive letters that form these words. Below is an example of the word **'bots'** and how to find its letters in the table:

b	a	s	i	n	d	i	v	i	d	u	a	l	s
o	b	e	n	e	f	i	c	i	a	l	u	n	w
t	h	c	o	m	p	a	n	i	e	s	t	g	e
s	g	u	d	i	g	i	t	a	l	e	o	l	b
r	e	p	e	t	i	t	i	v	e	n	m	o	s
f	o	m	e	s	s	a	g	e	z	g	a	b	i
a	m	a	l	i	c	i	o	u	s	i	t	a	t
s	k	s	o	c	i	a	l	h	j	n	e	l	e
t	d	s	e	a	r	c	h	b	k	e	d	c	x

Bots. - Automated. - Fast. - User. - Social. - Global. - Malicious. - Beneficial. - Repetitive. - Digital. Messages. - Website. - Search engines. - Companies. - Individuals.

Pay attention!

Web/content scraping

Content or web scraping, involves the automated downloading of a substantial portion or all of the content from a website, irrespective of the website owner's preferences, by automated bots. Content extraction bots are often used to repurpose content for malicious purposes, such as content duplication to enhance search engine rankings on websites owned by the attacker, violation of copyright, and theft of organic traffic.

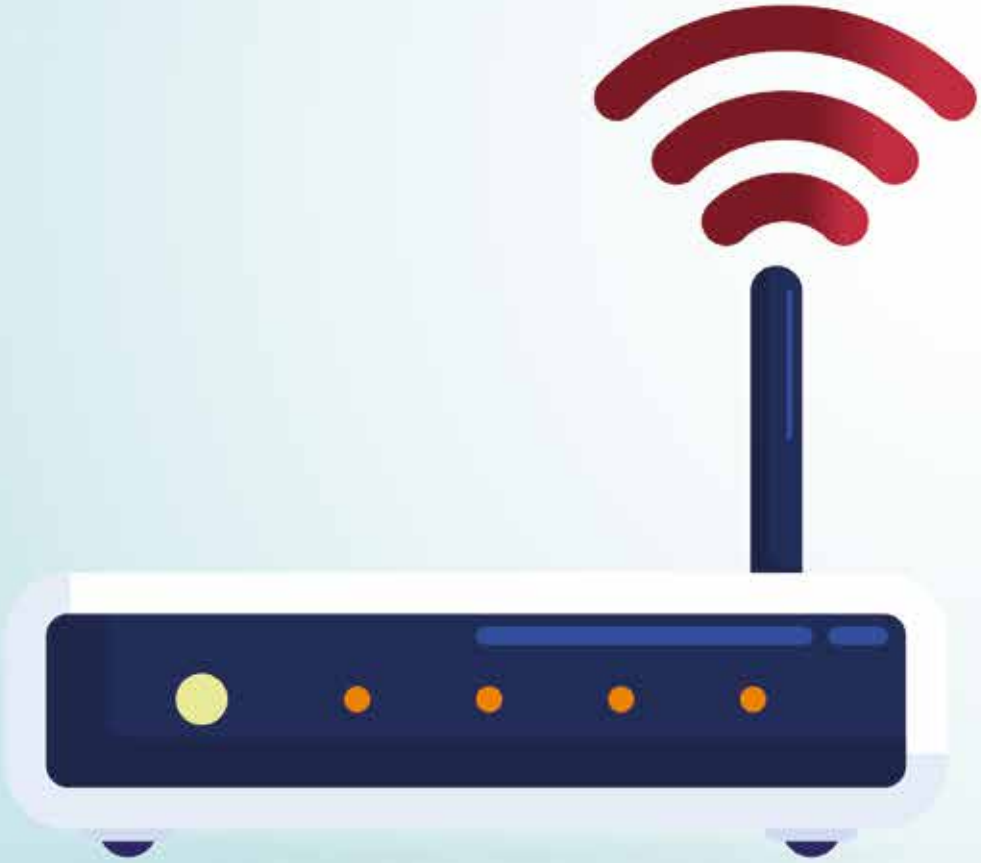
Pay attention!

Communication scraping

A type of malicious bot that scans websites to find contact information such as phone numbers and email addresses, and then downloading that information. Bots specializing in email scraping are considered a type of web scraping software that specifically targets email addresses, usually with the aim of discovering new targets for spam emails.

Did you know that...?

Slow internet speed is considered a sign of devices and files being infected by botnets



Pay attention!

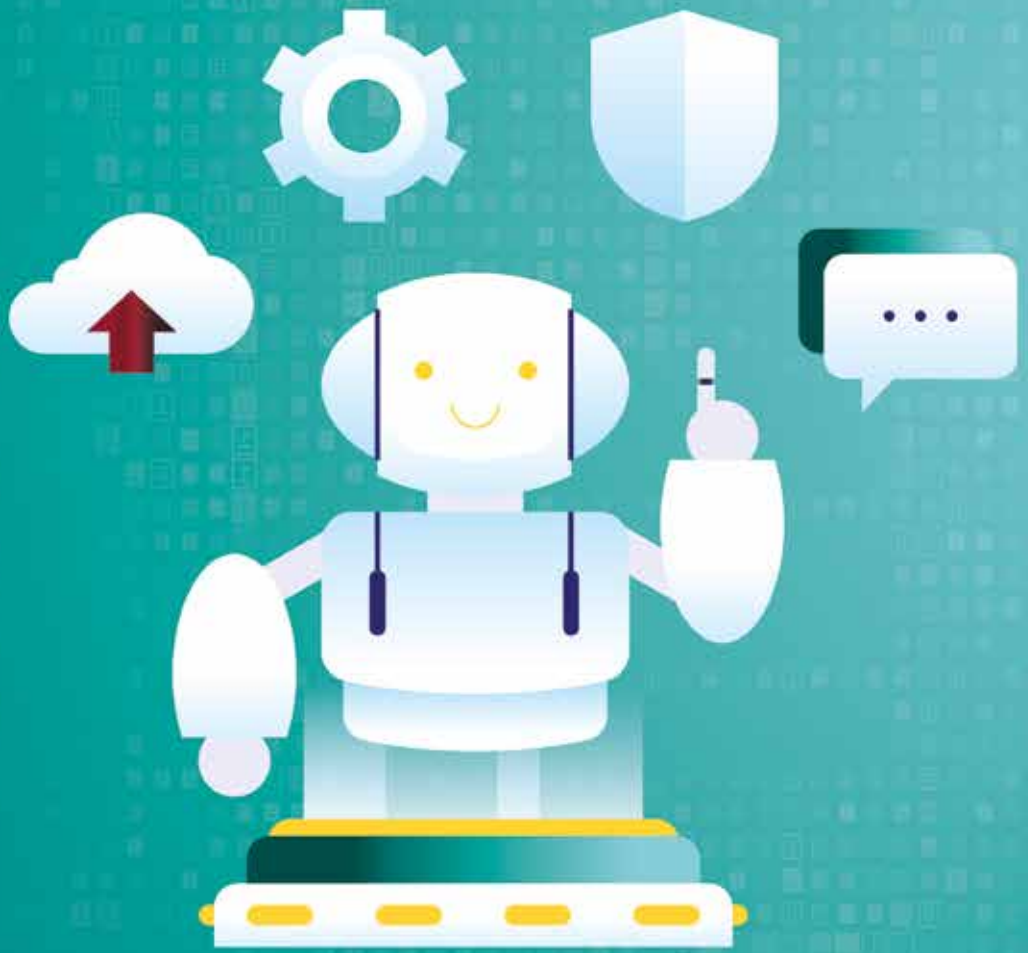
Bot management

Bot management refers to blocking the traffic of unwanted or malicious bots on the Internet while allowing access to beneficial bots to web properties. Bot management achieves this by detecting bot activity, distinguishing between desired and undesired bot behavior, and identifying sources of unwanted activity.

Pay attention!

Bot Manager

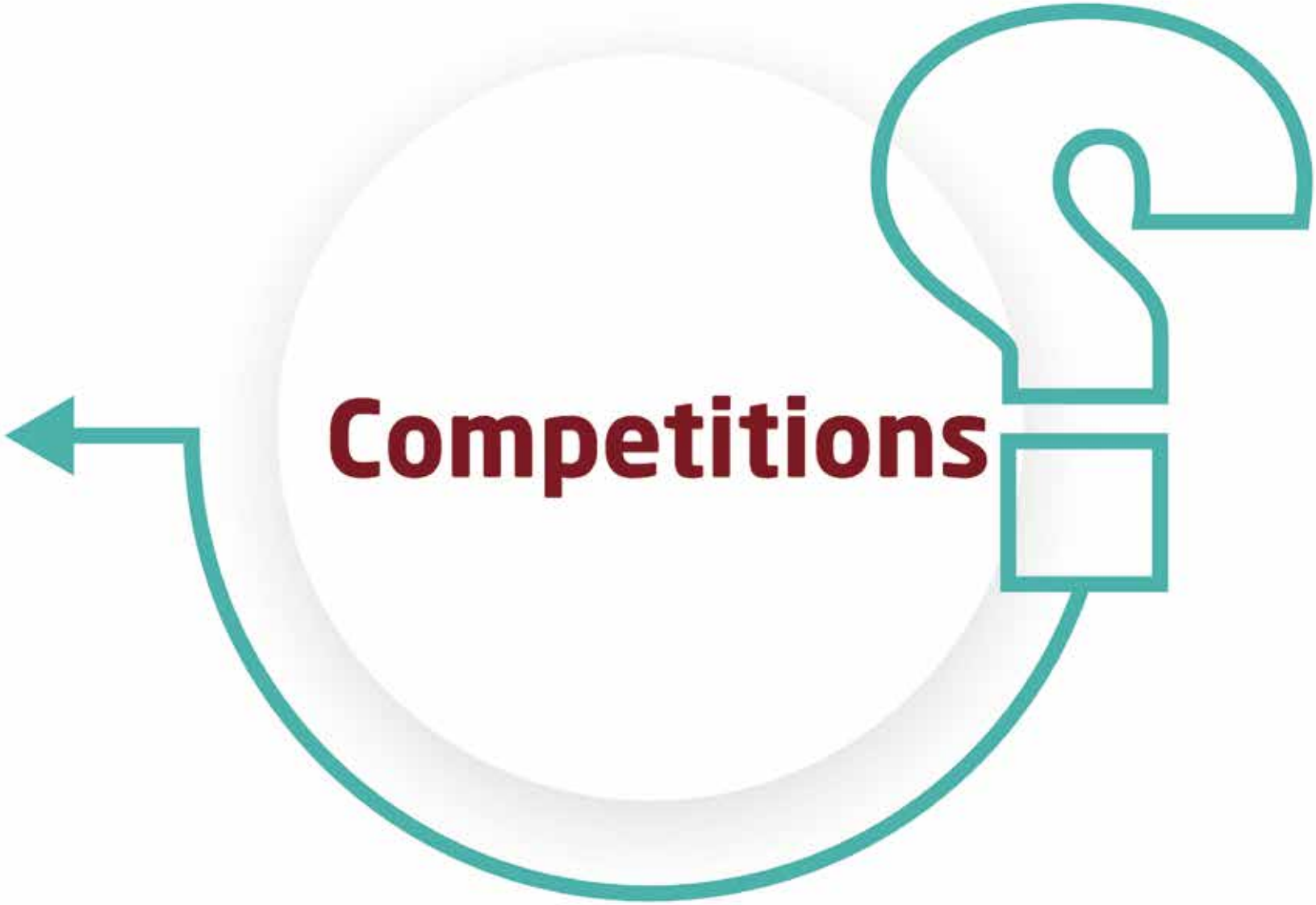
It is a software product that manages bots, where bot managers can block some bots and allow others to pass, instead of simply blocking all non-human traffic; because if all bot programs like Google bot are blocked and cannot index a page, that page will not appear in Google search results; resulting in a decrease in the number of visits to the website.



Pay attention!

Robots.txt file

It is a file located on a web server that outlines rules for bot access to the properties on that server. Anyone programming a bot should ensure that their bot checks the robots.txt file of the website before accessing it. Naturally, malicious bots do not adhere to this system, hence the need for bot management.


Competitions

What is it?

A program that performs automated, repetitive, and predetermined tasks. Typically mimic or replace human user behavior, but they operate much faster than humans.

They are internet-connected devices, each of which runs one or more bots, often without the knowledge of the device owners, since each device has its own IP address. So, it is difficult to determine the source of its traffic.

It is a bot designed to participate in conversations with users, typically through text or voice interfaces, using technologies such as Natural Language Processing (NLP) and Artificial Intelligence (AI).

This type of bots concentrates on repetitive tasks, data processing, and other routine activities that could consume a significant amount of time for humans.

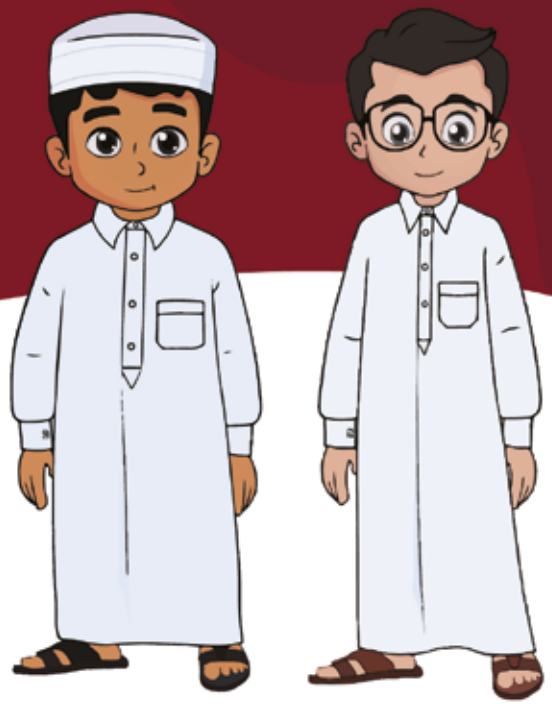
It can send unwanted messages to targets, such as spamming software that launch phishing attacks or disseminate negative comments on social media platforms to tarnish the reputation of a specific brand or company. Similarly, it can be employed for the illicit promotion of products or services.

A type of bots that distribute malicious software, such as Ransomware, viruses, Trojans, worms, and others, by exploiting vulnerabilities in the targeted systems.

It is a file located on a web server that outlines rules for bot access to the properties on that server.

Refers to blocking the traffic of unwanted or malicious bots on the internet while allowing access to beneficial bots to web properties by detecting bot activity, distinguishing between desired and undesired bot behavior, and identifying sources of unwanted activity.

Choose the correct answer:



1- Web bots are also referred to by other names such as ..... .

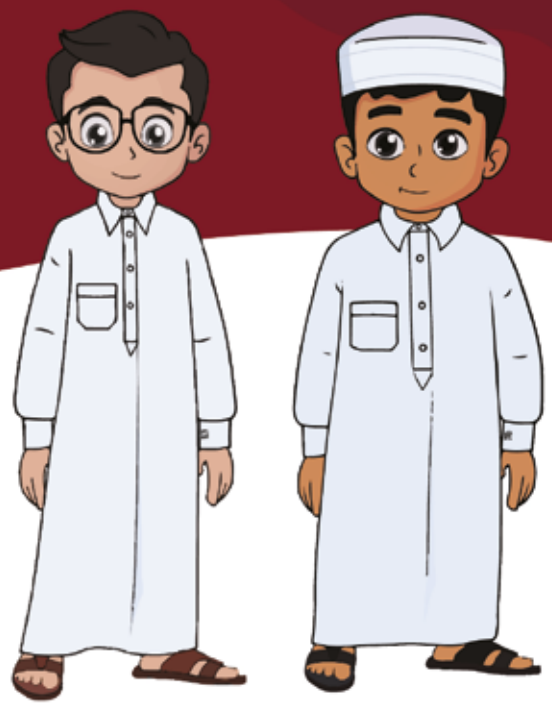
- ☐ Spiders
- ☐ Crawlers
- ☐ Web bots
- ☐ All of the above

2- Bots are divided into.... .

- ☐ Malicious bots
- ☐ Beneficial bots
- ☐ Neutral bots

3- One of the most common ways through which bots infect your computer is.... .

- ☐ Copying
- ☐ Downloading
- ☐ Transferring



4- Bots are considered crucial in the digital ecosystem for a number of reasons, including..... .

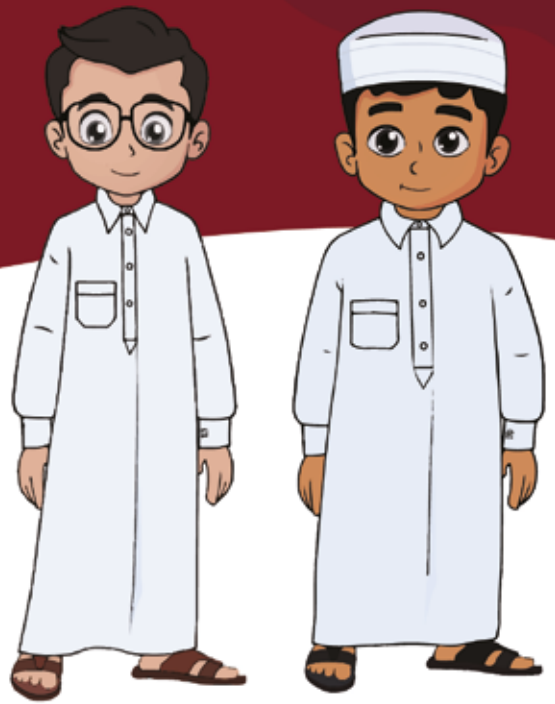
- [ ] Generalization
- [ ] The ability to execute a single task in a non-repetitive manner.
- [ ] Working around the clock

5- Beneficial bots include ..... .

- [ ] DDoS bots
- [ ] Spam Bots
- [ ] Backlink checker bots

6- Backlinks are considered important for ..... .

- [ ] Search Engine Optimization (SEO)
- [ ] To automate tasks on social media platforms
- [ ] To crawl the internet and find the information



7- Objectives of a good bot manager include ....

- ☐ Analyzing the behavior of the bot
- ☐ Adding malicious bot programs to the allowed lists
- ☐ Not limiting the excessive use of bots for service
- ☐ Allowing malicious bots access to specific content

8- to prevent bots attacks:

- ☐ click on all INTERNET links
- ☐ download all e-mail attachments
- ☐ make WI-FI allowance for all
- ☐ frequently update operating system and other applications

9- Indications of devices and files being affected by the botnet include ..... .

- ☐ An increase in processing speeds
- ☐ Not experiencing frequent application crashes
- ☐ Slow internet speed

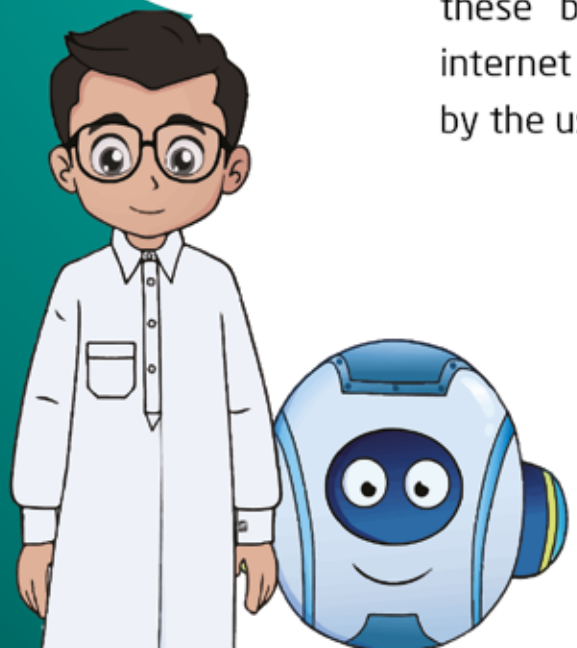
Compose the appropriate word from the letters provided in the table

Malware scripts that automatically browse websites, fill out web forms, and illegitimately manipulate data on websites.

W	E	B	B	O
T	S	A	L	O
Y	B	B	A	L

Also known as web crawling programs, these bots are used to crawl the internet and find information needed by the users.

S	T	B	E
O	H	ENG	CH
R	S	INE	A



Also known as credential stuffing bots, these bots can gain access to user accounts by launching attacks that involve utilizing stolen usernames and passwords or infiltrating user accounts using sensitive information such as credit card details and banking information.

R	Th	U	A	E
K	O	T	O	U
CC	N	B	T	T
V	T	A	A	S

This bot is designed to purchase fast-moving products or services in large quantities, making it difficult for genuine customers to complete legitimate purchase transactions.

E	P	E	A
K	O	T	O
TIV	I	B	S
X	T	A	GH

These are bots designed to gather information from various sources and create comprehensive directories or content lists to provide users with up-to-date information about websites, companies, products, or services.

R	C	E	A
D	O	C	R
T	L	T	S
A	L	O	O

Graduation Project

A graduation project is a duty that you do alone or jointly with one or two of your colleagues through which you and under the supervision of the trainer perform one of the following duties:

- Write a short story, report or essay explaining the concept of Web bots.
- Play the role of the trainer and write general instructions to his colleagues or his family explaining to them what the web bots are.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency