

Web bots

Trainer's Booklet



CyberEco

معاً لنحمي السلامة الرقمية
Together to support digital safety



High School



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Web bots

High School

Training Kit

(Trainer's Booklet)

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

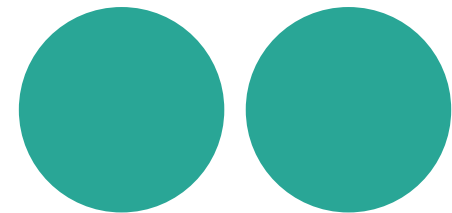
☎ 00974 404 663 78

☎ 00974 404 663 62

General content of the Kit

First: General Introduction to the training kit

Second: Scientific content



First: General Introduction to the Training Kit

Below is an explanation of some details relevant to the objectives of the training kit, along with general guidelines for the trainer on how to handle this kit, while providing him with the scientific content that will be relied upon during the training.

General Idea

The concept of this training kit is to equip the trainer with tools and training resources, making it easier for him to deliver information to the trainees. In general, each training material consists of two parts: One part for the trainee and another for the trainer. The training kit serves as a general guide and support for the trainer, and its scientific content is the same as that of the trainee, but here the training content is presented differently. Additionally, the kit equips the trainer with training tools and methods that support him in the training process.

Objectives of the Training Kit

- Providing the trainer with training tools that help him deliver the training content to the Trainees.
- To present information and training content in an easy and simple manner.
- To offer training content on protection of electronic devices along with multiple training tools and methods.

Contents of the Training Kit

The training kit includes several training tools, as detailed below:

1. **Presentation files.**
2. **Training games**, such as crossword puzzles, which the trainer presents to the students to ensure their interaction with the training content.
3. **Educational videos.**
4. **Competitions**, Contests in the form of inferential questions presented by the trainer to encourage interaction between the students.
5. **Training cards**, comprising general information accompanied by illustrative images, presented by the teacher to the students. Currently, the content of the training cards is being prepared, and will later be designed in the form of cards.
6. **Sketches**, including information about the main topics in the training content.

Content of the Training Kit

Introduction	17
--------------------	----

Chapter One

The concept of web bots and their types.....	19
--	----

- The concept of web bots.....21
- Types of web bots.....23
- Beneficial and malicious web bots.....30

Chapter Two

The operating mechanism of web bots and their benefits.....	41
---	----

- How do web bots operate?.....43
- What are the benefits of web bots?.....47
- Securing devices and files from malicious bots.....48

Exercices and Trainings.....	51
------------------------------	----

References	
------------	--

WorkShop Timetable

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	5 minutes
Total training time	2 hours

Trainer's Guidance Manual

The following is an explanation of some general guidelines for the trainer, revolving around how to use this training kit:

1. The scientific content of the kit may exceed the children's ability to comprehend, especially in terms of general concepts. Therefore, the trainer must simplify these concepts and present them in a way that is understandable to High school students.
2. The trainer presents slides for each point discussed. For example, when talking about the concept of web bots, the relevant slide is displayed.
3. During the explanation of the first chapter, specially designed images for the **"Did you know that..?"** section are distributed.
4. The trainer displays the **"Sketches"** section while the students are solving the exercises and exercises.
5. At the end of the training, the mentioned **competition questions** are presented.
6. During the presentation of the scientific material for each chapter, a portion of the allocated time is used to present several links related to the content of the chapter.
7. The trainer will show the videos -mentioned in a separate file- to the students at the end of each chapter, or when he sees it's appropriate.
8. It is encouraged to open a discussion with the students to hear their opinions.
9. Regarding exercises directed towards students; a file with exercises will be attached at the end of this kit. These exercises are divided into two parts: a part to be given to students during training, which are classroom exercises, and the other part assigned for students to answer at home, which are non-classroom exercises. This division will be explained at the end of this kit.

Graduation Project



The graduation project is a task carried out by the student, aimed at achieving several goals, Here is an explanation of the most important ones:

- Ensure that the student has absorbed the information and ideas presented and is capable of applying them in their daily life.
- Consolidate the information and ideas that were presented to the student.
- The project serves as a link between theoretical information and practical real-world application.
- The students choose the project topic, and the trainer can provide some assistance or ideas in this field.
- The topic of the graduation project must be consistent with the training content that was presented to the students.
- The graduation project can be within one of the following scenarios, which are non-binding concepts. The trainer can choose other concepts that he find suitable. Here are some suggestions:
 - Writing a short story, report, or article explaining what web robots are, and reviewing their most important advantages and disadvantages.
 - The student takes on the role of the trainer and writes general guidelines for his colleagues or parents, explaining web bots.

Regarding the mechanism for assigning students to the project, and how to implement it, the following guidance can be provided:

- The graduation project can be individual or group-based, In case of a group project; the number of students participating in one project should not exceed three students.

Second: scientific content

Introduction

The Internet is a vast world and an essential source of information and data due to the ease of access it offers through search engines. In cases where users are unaware of the specific page link leading to the information they seek, they turn to search engines to save time and effort. Search engines, such as Google, act as our gateway to the vast realm of the Internet, enabling us to access information available on websites sorted according to the most pertinent results for the search query. Search engines perform three primary functions: crawling, indexing, and ranking.

Crawling is the exploration process employed by search engines, which involve deploying teams of robots to uncover search-worthy content. The term robots refer to computer programs that systematically browse the Internet and are also known by various names, including: web crawlers, spiders, or web bots.

The content that bots search for exists in a variety of formats, including web pages, images, videos, and PDF files... In addition, all of these formats are discovered by bots using URL links. The bot then begins to gather pages and links, adding them to the index of a search engine such as Google. This content is then processed and arranged into a large database in its final form. The database is later referenced to extract the appropriate link when users search for a specific topic using search engines such as Google.

However, there are two types of bots: beneficial ones that provide useful services to users without causing harm to devices or systems and malicious bots that lead to breaches, exposing devices and files to cyber-attacks, such as Ransomware, spam and other forms of malicious activity.

Chapter One

The concept of web bots and their types

- First: The concept of web bots
- Second: Types of web bots
- Third: Beneficial and malicious web bots



0

1



First: The concept of web bots

The term “bot” is an abbreviation of “robot” and refers to 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 ⁽¹⁾. These are known as Internet bots, also known: spiders, crawlers, or web bots.

Today, up to half of all internet traffic is driven by computer bots, which perform specific tasks such as automating customer service, mimicking human interaction on social media, helping businesses find content on the internet and helping to improve search engine rankings. While individuals and enterprises today rely on bots to complete repetitive tasks that would otherwise be done by humans, as they can do them faster, bot programs can also be programmed to be malicious.

1. What are bots? - Definition and Explanation, Kaspersky, on site: <https://cutt.us/eX64R>

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.

Malicious bots 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.

One of the most common ways that bots infect your computer

is through downloads. 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. This can lead to a number of risks, such as: Data theft and identity theft, logging sensitive information such as passwords, banking details and addresses, and phishing.

Malicious bots can go undetected, as they can easily hide within a computer. They often have file names that resemble files that are already on the device.

Web bots

These are malware scripts that automatically browse websites, fill out web forms, and illegitimately manipulate data on websites. The relentless threat of web bots can lead to serious issues in web applications.

According to various web traffic reports, more than 50% of total web traffic comes from web bots. Effective protection against automated web bots involves detecting the presence of a human user on web applications. Most current research focuses on detecting specific web bots, such as form spam bots, data scraping bots, chat bots, and gaming bots.⁽¹⁾

1. Rizwan Ur Rahman & Deepak Singh Tomar. New biostatistics features for detecting web bot activity on web applications, , 2020, on site: on site: <https://cutt.us/MtBbH>

Second: Types of web bots

Bots are software applications designed to automate specific tasks and interact with users, often mimicking human conversation when it comes to chatbots. They are programmed to follow pre-defined rules or use artificial intelligence (AI) algorithms to process human language and generate responses.

Bots are considered crucial in the digital ecosystem for a number of reasons, the most important of which are:

- 1. Efficiency:** bots can handle repetitive and routine tasks much faster than humans, increasing overall efficiency and productivity.
- 2. Personalization:** Advanced bots with artificial intelligence capabilities can learn from user interactions, providing personalized experiences over time.
- 3. Availability:** Bots can work 24/7, providing immediate assistance to users without the need for human intervention.
- 4. Low cost:** By performing tasks, bots can help reduce labor costs and improve resource allocation.
- 5. Scalability:** Bots can handle multiple interactions at the same time, making them ideal for dealing with large volumes of inquiries or operations.

Types of bots

Bots are designed to perform specific tasks autonomously with varying degrees of complexity. They can be found in a variety of contexts ranging from social media platforms to websites, customer service interactions, e-commerce, data collection and more. **Bots are generally divided into two main types:**

1. Chatbots:

They are 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.



2. 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 there are several types of good bots:

• Search engine 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 they need. And these bots crawl and index the web to improve the efficiency of search engine queries and their searchability; some examples include: GoogleBot, Bingbot, DuckDuckGo, and Amazonbot.

• Backlink checker bots

Backlinks are crucial for search engine optimization (SEO) as they can aid in enhancing a website's rank in search results. Backlink checker bots can assist in identifying backlinks for a specific web page, evaluating their progress and quality, and verifying the quality of existing backlinks. This allows users to enhance the web page's ranking. For example, these bots include: Ahrefs, Botster, and Ninja SEO.

• Social media bots

These bots are designed to automate tasks on social media platforms. As it can perform the following tasks:

- Creating and publishing social media posts.
- Collecting user information
- Providing customer support.
- Tweeting constantly.

Bots can also be used for malicious purposes, such as sending spam on social media.

• Chatbots

Chatbots are a common type of web bot. Their main purpose is to provide customer support 24/7 for products or services. These bots can provide a pre-defined set of frequently asked questions (FAQs)

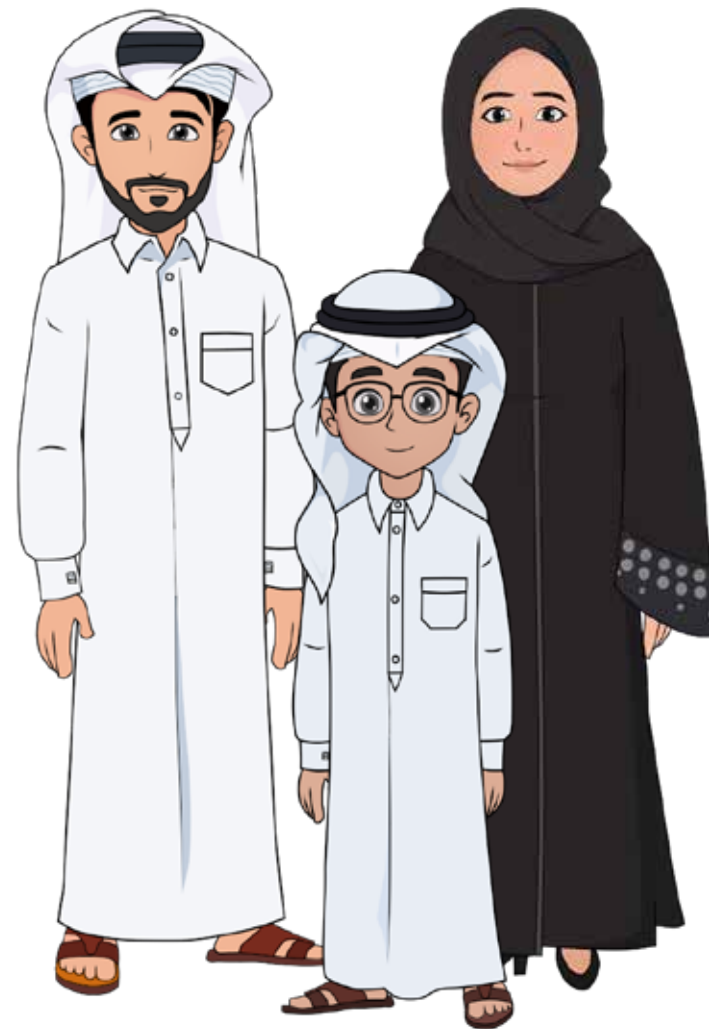
and guide users through completing specific tasks, which allows companies to improve their customer support.

- **Game bots**

Game bots are specifically designed to perform game-related activities such as simulating human players in multiplayer games, providing game information, and testing games.

- **E-commerce bots**

They are considered a type of chatbot that helps promote products or services by providing product recommendations and assistance with purchases. ⁽¹⁾



1. Shanika Wickramasinghe. Bot Types 101: Bad Bots, Good Bots and Everything in Between, July, 2023. On site: <https://cutt.us/i3Njc>

Malicious bots

These bots are designed to engage in a variety of harmful activities, and they pose a serious threat. Malicious bots can function as malware, exploiting vulnerabilities to gain unauthorized access to user accounts. Malicious bots can also target specific enterprises to tarnish their reputation on social media by disseminating fake news or sending random emails to everyone they know. These bots are used by cybercriminals or anyone seeking to exploit vulnerabilities in targeted users.

Malicious bots types

1. DDoS bots

These bots are designed to launch Distributed Denial of Service (DDoS) attacks on websites, networks, or servers. As they send a large volume of traffic to the target that it cannot handle, rendering it unavailable to legitimate users.

2. Spam bots

Spambots can send unsolicited messages to targets. For instance, spamming software may orchestrate phishing attacks or posting 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.

3. Account takeover (ATO) bots

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

4. Malware distribution bots

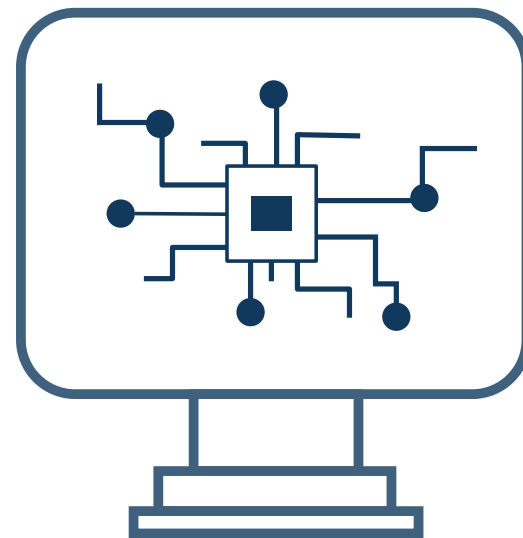
These bots have the capability to distribute malicious software, such as ransomware, viruses, trojans, worms, and others, by exploiting vulnerabilities in the targeted systems and spreading the malicious programs.. Once the system is afflicted with malicious software, it may carry out various harmful activities, such as encrypting files, stealing sensitive data, and spreading the malicious programs to other parts of the system.

5. Exploitative bots

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. Subsequently, these bots can resell the acquired goods or services through resale on websites at a higher cost.

6. 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.

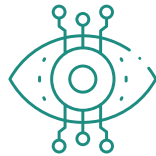


Risks of malicious bots

The risks and damages posed by malicious bots manifest through several negative effects. **The following outlines the most significant among them:**



1) Manipulation of content: Manipulation of content: Bots can be employed to manipulate online discussions and trends on social media platforms, leading to the dissemination of misinformation or creating a distorted perception of public opinion.



2) Violations of data privacy: Bots may exploit vulnerabilities in systems to gain unauthorized access to sensitive user data, leading to privacy violations and identity theft.



3) DDoS attacks Botnets, which are networks of compromised computers controlled by a single entity, are used to launch DDoS attacks against servers and disrupt services.



4) Diminution of trust: Malicious bot attacks can lead to a decline in user trust in online platforms and companies, which can impact their engagement.



5) Fraud and theft: Malicious bots can be utilised to execute fraudulent activities such as account takeover, theft of personal identification information, dissemination of fake reviews, or the spread of misleading information.

Third: Beneficial and malicious web bots

In the context of web security, bots can be broadly classified into two main categories: Beneficial and malicious. Within each category, there are various types of bots. While all bots can perform similar actions, such as accessing web resources (pages, web applications, application programming interfaces, etc.) or engaging in other activities similar to human users, their purposes and intentions vary significantly. Therefore, understanding the different types of bots is of paramount importance for effective web applications and secure application programming interfaces. **The following outlines the most important types of beneficial and harmful malicious.**

• 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, **and the most important bots in this category are web crawlers and data collectors.**

1. Web crawlers (web crawling programs):

Web crawlers, also known as web crawling programs, are deployed by search engines to index web content and update their search results. These bots crawl websites, gather information, and index it in the search engine's database. Generally, website owners welcome web crawlers because they assist in increasing visibility on search engines and attracting more users and customers. They are referred to as 'web crawling programs' because crawling is the technical term for the automated access to a website and the retrieval of data through software.

These bots are consistently operated by search engines through the application of algorithms on the data collected by web crawling programs. Search engines can provide relevant links in response to user search queries and generate a list of web pages that appear after a user types a search into Google or another search engine.

That process closely resembles individuals browsing through all the books in an unorganized library and conducting card cataloging to enable anyone visiting the library to quickly and easily find the information they need.

≡

How do web crawling programs operate?

Web crawling bots start from a list of known URLs, initially crawling web pages at these addresses. While crawling these web pages, they discover branching links to other URLs and add them to the list of pages that will be crawled subsequently.

Given the vast number of web pages on the internet that can be indexed for search, this process can continue indefinitely, approximately. However, the web crawler follows specific policies

that make it more selective about the pages it will crawl to verify content updates.

The significance of this type is that a web page referenced by many other web pages, and which receives a substantial amount of visitors, is likely to contain reliable and high-quality information. Therefore, it is particularly important for the search engine to index it, much like how libraries ensure the retention of multiple copies of books that are frequently reviewed by many individuals.



List of web crawling programs

The bots in major search engines are referred to as:

Google: In fact, there are two crawling programs for Google, Googlebot Desktop and Googlebot Mobile, for desktop and mobile search operations.

Bing: Bingbot

Yahoo! Search:
Slurp

Yandex:
YandexBot

Baidu: Baiduspider

Exalead
ExaBot⁽¹⁾

There are also numerous other web crawling bots, some of which are not associated with any search engine.

1. What is a web crawler bot? Cloudflare. On site: <https://cutt.us/SWZvK>

2. 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.



- The definition of data bots is as follows:

It is a set of technologies and applications that are necessary to design and implement a new level of process automation based on artificial intelligence (AI), machine learning, and other technologies. It aims to improve productivity and efficiency in business processes.⁽¹⁾

1. Types of bots. An In-Depth Guide by Redware. On site: <https://cutt.us/dN7Wo>

• Malicious bots

Malicious bots pose a significant threat to web security as they are deployed with malicious intent, or at least for purposes that may not necessarily be in the best interest of the owners of web resources. They target web applications, application programming interfaces, and websites, causing varying levels of damage and potential serious consequences. They constitute a significant part of web traffic today, and there are numerous types of malicious bot attacks that represent a diverse range of threats.

What is a 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. Bot attacks can lead to the destruction of business operations for enterprises, loss of revenue, and damage to reputation.

Types of bot attacks

1. Credential stuffing

It is a type of cyber-attack in which compromised credentials obtained from a data breach in one service are used to attempt unauthorized access to another unrelated service. For example, an attacker might take a list of usernames and passwords obtained from breaching a major retailer and use the same login credentials to attempt to log in to an account on a local bank's website. The hope is that some customers of the store also have accounts with the bank and reuse the same usernames and passwords for both services.

This bot spreads widely thanks to the massive lists of compromised credentials circulated and sold in the black market. Credential stuffing attacks have a very low success rate; out of every thousand accounts an attacker tries to compromise, they will succeed approximately once. If an attacker has a million sets of credentials, this can lead to successfully compromising around 1000 accounts. Modern credential

stuffing attacks circumvent these protective measures by using bots to attempt multiple login operations simultaneously, appearing to come from a diverse range of device types and originating from different IP addresses. It is worth noting that the malicious bot's goal is to make login attempts by the attacker indistinguishable from normal login activity. The primary reason behind the effectiveness of credential stuffing attacks is that people tend to reuse passwords⁽¹⁾.

2. Web/content scraping

It occurs when bots download content from a website to use it in future attacks. A bot sends a series of requests to extract information from a website, copying the data and saving it all within seconds. 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. Web scraping bots interact with websites and application programming interfaces as if an individual were using a conventional web browser, attempting to deceive the web server into believing that a human user is accessing the content.

Attackers can use the stolen data for various purposes, such as reusing text on another website to steal the ranking of the first site in search engine results. They may also deceive users or create fraudulent phishing websites that trick users into entering personal information by appearing as a legitimate version of another website.



1. What is credential stuffing? | Credential stuffing vs. brute force attacks, Cloudflare. On site: <https://cutt.us/GpCSq>

And among the types of this malicious bot are:

- **Communication scraping**

This refers to scanning 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.

- **Price scraping**

This occurs when a company downloads all pricing information from a competitor's website, enabling it to adjust its own prices accordingly ⁽¹⁾.

3. 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 by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks achieve their effectiveness by utilizing compromised computer systems as sources for the attack traffic. These attacks are executed using networks of internet-connected devices, which include computers and other devices (such as Internet of Things devices) that have been infected with malicious software, allowing the attacker to control them remotely. These individual devices are commonly referred to as bots (or zombies), and are collectively known as a "botnet." Once a botnet is established, the attacker gains the capability to orchestrate the attack by remotely sending instructions to each bot.

When a server or victim's network is targeted by a botnet, each bot sends requests to the target's IP address, potentially causing exhaustion of the server or network resources, leading to a denial of service for legitimate traffic. Since each bot represents a legitimate internet device, it can be challenging to distinguish attack traffic from normal traffic ⁽²⁾.

1 . What is content scraping? | Web scraping. On site: <https://cutt.us/N1xas>

2. What is a DDoS attack? On site: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

4. 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. Brute-force attacks on passwords are often executed through scripts or bots targeting the login page of a website.

What distinguishes brute-force attacks from other hacking methods is that they do not employ a strategic approach; rather, they simply attempt to use different sets of characters until the correct one is found.

Strengths and weaknesses in brute-force attacks

One of the significant advantages of brute-force attacks is that they are relatively easy to execute and time-efficient, hence they consistently succeed. It is possible to breach any password-based and encryption key-dependent system using a brute-force attack. On the other hand, brute-force attacks can be exceedingly slow, as attackers may need to go through every possible combination of characters before achieving their objective. This deceleration intensifies with an increase in the number of characters in the targeted sequence

(a sequence being simply a group of characters). For instance, a password consisting of four characters requires a considerably greater amount of time to be compromised compared to a three-character password, and a password composed of five characters necessitates a significantly longer duration than one comprised of four characters. Once the number of characters surpasses a certain point, imposing a truly random password becomes impractical. If the targeted sequence is sufficiently lengthy, a brute force attacker may spend days, months, or even years decrypting the randomly generated password accurately.

Preventive Measures against Brute Force Attacks

Web services users can mitigate their vulnerability to brute force attacks by opting for longer and more complex passwords. It is also advisable to enable two-factor authentication and use unique passwords for each service. If an attacker manages to compromise a user's password for one service, they may attempt to recycle the same login information and password across several other common services. Users should also refrain from 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⁽¹⁾.

1. What is a brute force attack? On site: <https://cutt.us/YYbNT>

5. Click Fraud

Click fraud occurs when fraudulent clicks are directed towards pay-per-click advertisements, manipulated to enhance search engine rankings for a web page, or artificially inflate the popularity of a post on social media. Often, click fraud is orchestrated by click bots, where 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. Click fraud typically occurs on a broad scale, with multiple clicks on each link, not just once, and targets multiple links. Fraudsters utilize bot programs that repeatedly click.

Motivations for Click Fraud

01

Most often, especially with advertising fraud, fraudsters seek to achieve financial gains.

02

For enterprises, the aim is to undermine the advertising budgets of their competitors.

03

The manipulated likes or positive voting for a particular post are aimed at making certain emotions appear more popular than they actually are.

04

Internet criminals can employ click fraud to elevate a malicious web page's visibility in search rankings, making it appear legitimate.

Common Types of Click Fraud

- 1. Advertising fraud** occurs when a website operator attracts fraudulent clicks on pay-per-click advertisements on their website.
- 2. Perpetrators of fraud can create web pages** displaying advertisements through clicks, then utilize click bots to 'click' on those advertisements. With each click, the advertising network is obligated to pay the website operator (the fraudster). As a result, the more fraudulent clicks increase, the advertising network is compelled to pay the website if the fraud is not detected.
- 3. Advertising fraud can also constitute a financial attack on the company** that pays for the advertisements. Fraudsters target pay-per-click advertisements on websites they do not own. Here, the fraudster does not seek to profit from the clicks. Instead, the targeted company is obligated to pay the advertising network for each click, incurring financial costs for them.
- 4. Manipulating search engine rankings** by artificially increasing

the click-through rate. Click-through rate refers to the number of users out of the total page visitors who click on a specific link. Considering that the click-through rate is one of the ranking factors taken into account by search engines such as Google, the objective of this attack is to increase the click-through rate for a web page, thereby boosting the search engine ranking and attracting more visits from genuine users.⁽¹⁾

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, and varying the timing between each click, and so forth.

By employing this method, the fraudster who wrote the bot hopes to present the bot clicks as if they are originating from legitimate users. Since hundreds or thousands of clicks from a single device

1. What is click fraud? On site: <https://cutt.us/zD5On>

may appear suspicious immediately, fraudulent clicks often involve bot programs installed on multiple devices. And each of these devices has a different IP address, hence, making each click appear to come from a distinct user. This network of devices is known, where each device runs a copy of the bot, under the name of the botnet.

Botnets comprise thousands or even millions of user devices where bot software has been installed. Most of the time, it operates without the users' knowledge as a result of the device being infected with malware. For instance, 'Clickbot.A' was a click fraud botnet that affected over 100,000 user devices.

Does click fraud only occur from bots?

While bots are commonly used to carry out fraudulent click operations, 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 migrate 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.

Losses from Click Fraud

Estimates indicate advertisers incurred losses of \$19 billion due to fraud in 2018 alone. In a long-term fraudulent operation uncovered in late 2018, a single criminal organization earned over \$29 million through advertising fraud. Similarly, companies managing pay-per-click (PPC) advertising campaigns may find themselves paying for fraudulent clicks generated by bots. For instance, in 2016, marketers lost \$7.2 billion due to advertising fraud ⁽¹⁾.

Additionally, click fraud can lead to disruptions in website analytics. If bots interact with a website, their activities will be included in the data, making it difficult for website operators to accurately measure the effectiveness of a displayed ad or assess the genuine behavior of real users. Consequently, they cannot gauge the success of their content in engaging the audience.

1. What is click fraud? On site: <https://cutt.us/zD50n>



Chapter Two

The operating mechanism of web bots and their benefits

- How do web bots operate?
- What are the benefits of web bots?
- Securing devices and files from malicious bots.



How do web bots operate?

Web bots operate based on a set of principles and foundations.

The following is an explanation of the most important ones:

- **Application logic:** It is the executable and automatically readable code written by the bot developer and executed by the computer. The example code of the chatbot above falls into this category.
- **Database:** It is the dataset from which the bot derives information about the actions to be taken. Here, the bot can store additional information in its own database, as is the case when a web scraping bot downloads content from a website.
- **API Integrations:** Application programming interfaces enable the bot to utilize external functions without the developer having to write them. All the developer has to do is add the correct commands to the code, and then the bot calls the application programming interface (API) as needed.

In other words, the Application Programming Interface (API) 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 (API)⁽¹⁾

What are the functions of bots?

Bots can essentially perform any repetitive and non-creative task, meaning anything that can be automated. They can interact with web pages, fill out and submit forms, click on links, scrape or "crawl" text, and download content. Additionally, bots can "watch" videos, post comments, and share or like or retweet on social media platforms. Moreover, some bots can engage in conversations with human users, a functionality commonly known as chatbots.

1. What is click fraud? On site: <https://cutt.us/zD5On>

How websites and applications deal with excessive bot traffic

Bots are extremely common on the internet, with approximately half of the total internet traffic coming from bots, whether they are beneficial or malicious. Some bots, such as web crawling bots and chatbots, are essential to help the internet function correctly and allow users to find the information they need. However, excessive bot traffic can overwhelm the original servers of the website. And thus, malicious bots can execute various cyber-attacks. To prevent these cyber-attacks and excessive bot traffic, websites and web applications use robots.txt files to leverage bot management solutions.

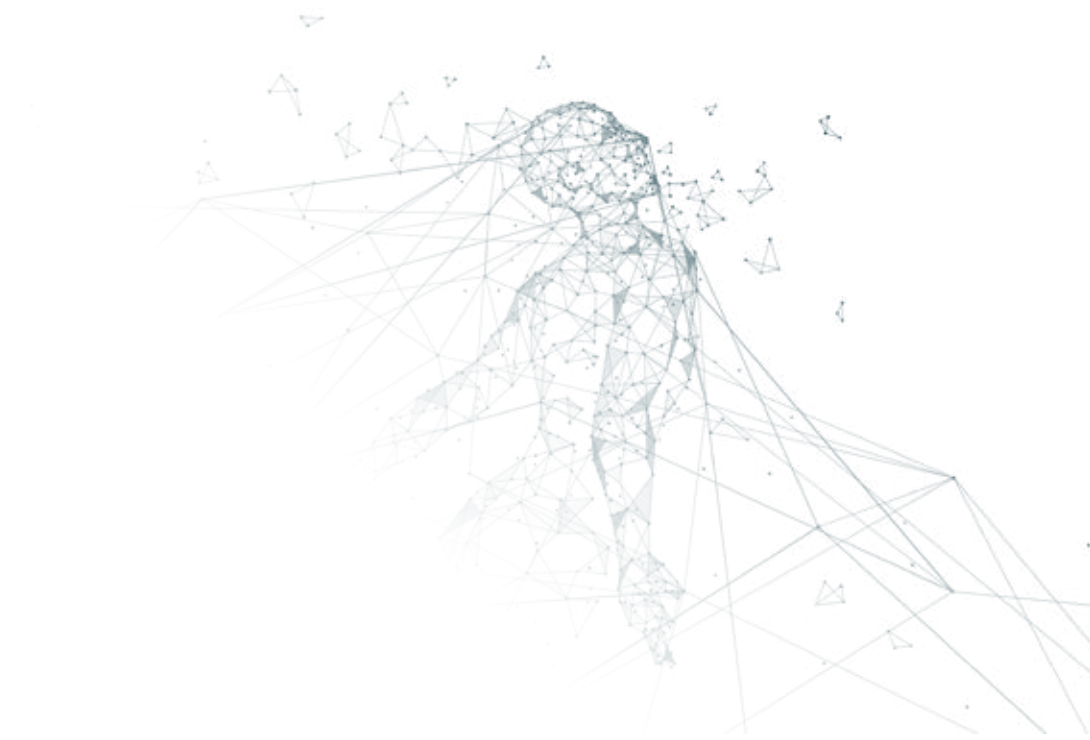
What is the robots.txt file?

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. Malicious bots do not adhere to this

system, hence the need for bot management.

Bot management

Bot management includes identifying and blocking certain bots from a website or application while allowing access to others. Bot management works to block unwanted or harmful bot traffic on the internet, allowing beneficial bots to access web properties. It achieves this by detecting bot activity, distinguishing between desired and undesired bot behavior, and identifying sources of unwanted activity.



The importance of bot management becomes evident in:



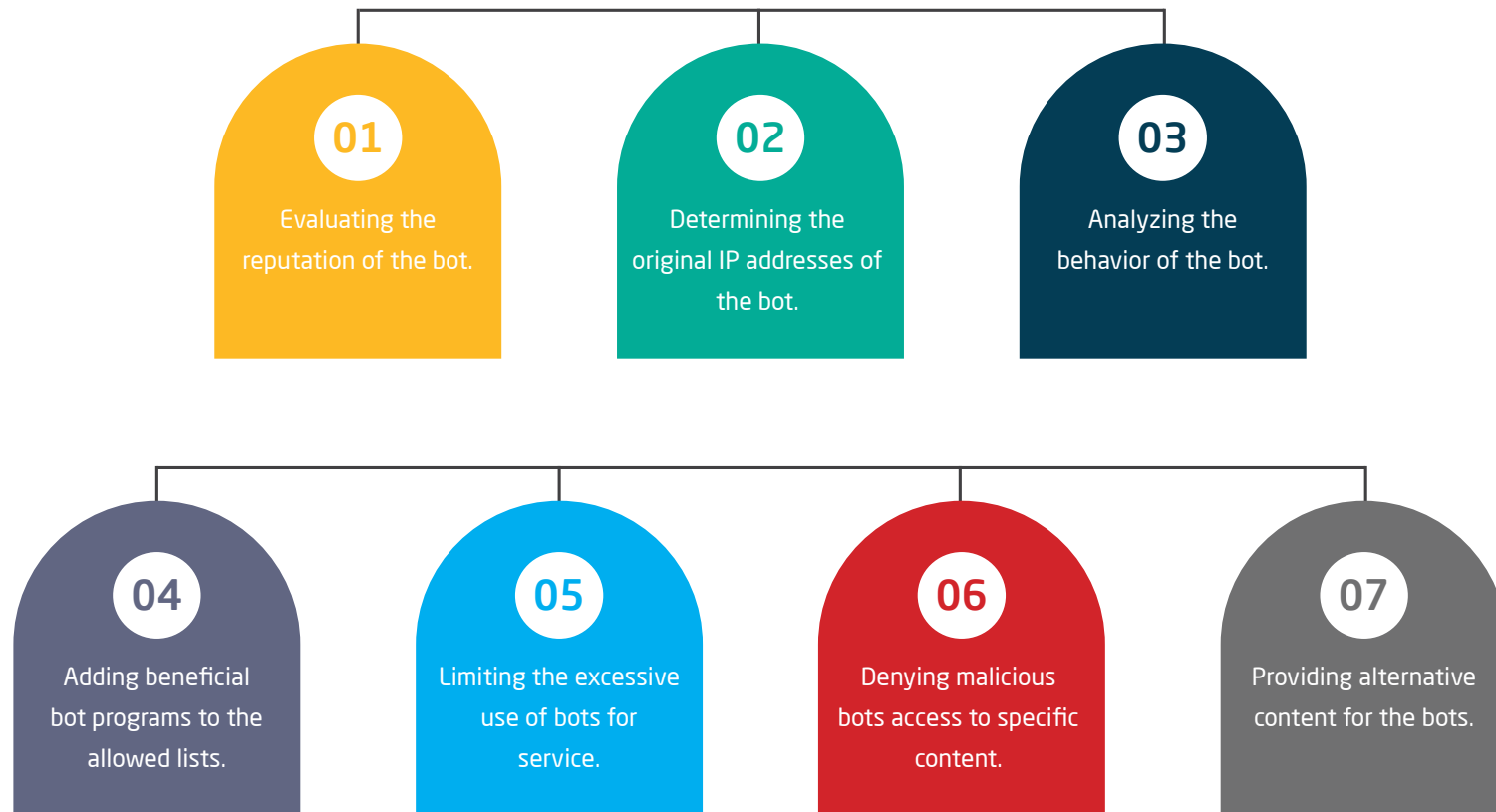
- In the case of leaving bot traffic undefined, it can cause significant issues for web properties.
- The very substantial traffic of bots can lead to an increased load on web servers, causing service slowdowns or denials for legitimate users ⁽¹⁾.

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.

1. What is bot management? | How bot managers work, Cloudflare. On site: <https://cutt.us/5cnit>

And the objectives of a good bot manager include:



What are the benefits of web bots?

1. Task automation:

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

2. Enhancing the efficiency of internet service:

The Bots operate around the clock without interruption, ensuring continuous service availability. For example, they can provide immediate responses to frequently asked questions, reducing response times and improving customer satisfaction.

3. Scalability:

Bots can handle a large number of simultaneous interactions, making them highly scalable solutions. This allows enterprises to meet the needs of a growing user base without the need for an increase in human resources.⁽¹⁾

4. 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.

5. Enhanced User Experience:

In e-commerce, chatbots can provide personalized assistance, guide users through processes, and suggest products or services based on their preferences ⁽²⁾.

1. Types of Bots: An In-Depth Guide by Radware, radware. On site: <https://cutt.us/Wee8j>

2. 7 Advantages of Robots in the Workplace, robotics tomorrow. On site: <https://cutt.us/ph64H>

Securing devices and files from malicious bots

Botnets are becoming increasingly sophisticated, and an ordinary user may not be aware of whether their devices are part of one of these botnets or not. **There are some signs indicating infection by a botnet, including:**

- 1.Decreased processing speeds:** Due to the utilization of processing power by botnets to achieve their objectives, the solution is to visit the task manager or activity monitor on your device to identify the applications and services using processing capacity.
- 2.Frequent application crashes:** If you notice frequent crashes of applications or programs on your device, it may be due to a decrease in processing capacity caused by bots.
- 3.Slow internet speed:** As the programmed botnet engages

in sending unwanted email messages or launching phishing attacks, it consumes the targeted user's internet bandwidth.

- 4.An increase in the number of unusual posts or email messages:** Bot developers work to expand their network by disseminating fake posts on social media or sending emails to your contact list. Therefore, an increase in the number of unusual posts or email messages from your accounts is a clear sign of being affected by a botnet.
- 5.At times, a botnet may install additional files and programs to increase its spread or install malicious software on your devices.** If you notice the presence of new and suspicious files or programs that you did not download or install, your device may be infected with malware associated with the botnet. It is also susceptible to infection by other types of malware, such as ransomware.⁽¹⁾

1. How to Block Bad Bots on Your Website - 4 Mitigation Methods. On site: <https://cutt.us/XINPY>

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

If you are experiencing some of the aforementioned indicators, it is highly likely that your device is infected with malware from a botnet.

And here, the following instructions must be followed:

- 1. Disconnect your device from any network;** this includes disconnecting it from the Wi-Fi network and disabling any Bluetooth connections to prevent the infection of other devices.
- 2. Identify malware using antivirus software,** or you can manually search for any suspicious files, but it is a laborious and very slow process. Furthermore, there is a chance of identifying the incorrect file.
- 3. By removing the malware automatically or manually,** the automatic method is preferred as it ensures the complete removal of infected files from your device.
- 4. If the indicators of malware infection from the botnet persist**

after taking the aforementioned instructions, it is advisable to reset the device and reinstall the operating system.

- 5. Report the infection of the botnet to the relevant authorities,** as despite removing the malware infection from your device, the botnet remains present and active. To prevent further damage, it is essential to report the infection to the relevant cybersecurity authorities⁽¹⁾

How to prevent bot Attacks?

Detecting malware in a botnet is not easy, **so it is better to prevent infection with a botnet by following the instructions outlined below:**

1. Avoid clicking on suspicious links; as most forms of malware spread through phishing links and spam emails.
2. Avoid downloading any email attachments from unfamiliar senders.
3. Do not download software or programs from unverified sources,

1 . What is a Botnet and How to Protect Your Devices in 2023? On site: <https://cutt.us/Xh56M>

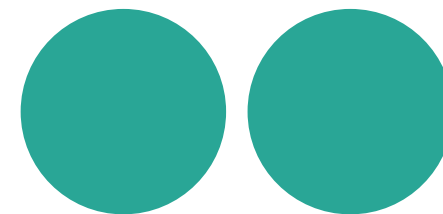
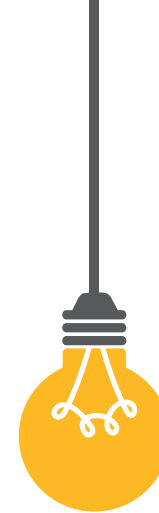
such as free software from the internet, as it may be part of a botnet.

4. Enable the firewall on your device, as this will help prevent downloads of files infected with malware, including malicious bot programs.
5. Change the default password settings on your smart devices, and ensure that the secure password typically consists of a combination of characters, numbers, and alphanumeric characters.

6. Keep your internet of things devices on a separate Wi-Fi network, as they are relatively easy targets for bot hackers. This can be achieved by maintaining internet of things devices on a different Wi-Fi network, either by creating a separate network on your router or by purchasing a new secure VPN router.
7. Set up a guest network on your Wi-Fi router to prevent the spread of infections from devices belonging to people within its range.
8. Regularly update the operating system and other software to ensure prompt access to patches and updates.
9. Install antivirus software⁽¹⁾.

1 . What is a Botnet and How to Protect Your Devices in 2023? On site: <https://cutt.us/Xh56M>

Exercises and trainings



- **Exercises are a major part of the training process, and they achieve several goals and aims, as follow:**
- Exercises are an effective tool to assess students' utilization of the training content and its impact on their cognitive inventory.
- They serve as a vital means to reinforce information and knowledge, constituting a rapid review of the training content
- They help to identify knowledge gaps among students.
- They act as a form of feedback for the trainer, providing information on the effectiveness of the training kit and the training method.
- During the training, after introducing an idea, the trainer will request students to open their respective booklet and answer the specific question, directly related to the presented idea or subject
- The exercises are carefully selected to be simple, easily understood, and solvable by middle school students. The trainer may offer support to students in answering some exercises if necessary, at their discretion.
- The exercises are divided into two parts; one for in-classroom use, called classroom exercises, and another is non-classroom, to be completed at home by the students.
- The answers for each exercise are provided, highlighted in a different color.

Approach to Dealing with Exercises:

The exercises mentioned in this section are comprehensive of the training content in this kit, here's an outline of the proposed methodology for dealing with them:

Below is an explanation of exercises specific to Middle school students, arranged according to chapters and classified as in-classroom and homework exercises (Non-classroom Exercises). These exercises, in the form presented here, are the same as those in the students' booklet.



First: **in-classroom Exercises**

The exercises here are accompanied by the answers, while in the student's booklet they are written without a solution, and are accompanied by guidance for the student on how to solve, when necessary.

Exercise I

Complete the following sentences:

1. Internet bots are known as**Web bots**..... or.....**Bots**..... of net.
2. Web bots undertake automatic.... **tasks**..... online, forming part of ..**programs**.. handling ...**complex**...and intricate tasks ..**automatically**..
3. Web bots carry out both simple and complex tasks repetitively at a rate ...**higher**... than what ...**humans**... can achieve.
4. The primary mission of web bots is**to search**... Web pages, as they are responsible for extracting and ...**collecting**..information from web servers ...**promptly**..... and ...**more**... swiftly than**humans**..
5. Each server possesses file...**digital**... for indexing, encompassing all the regulations dictating the behavior of**the bot**..... on that server.





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

7. Social bots also monitor chat **...rooms..** and **..conversations..** designed for interacting with **..Internet...** users.

8. **...Bots...** on social media platforms are designed to emulate **..human behaviors..** to collect patterns **..Behavioral..** similar to user pattern.





Pay attention!

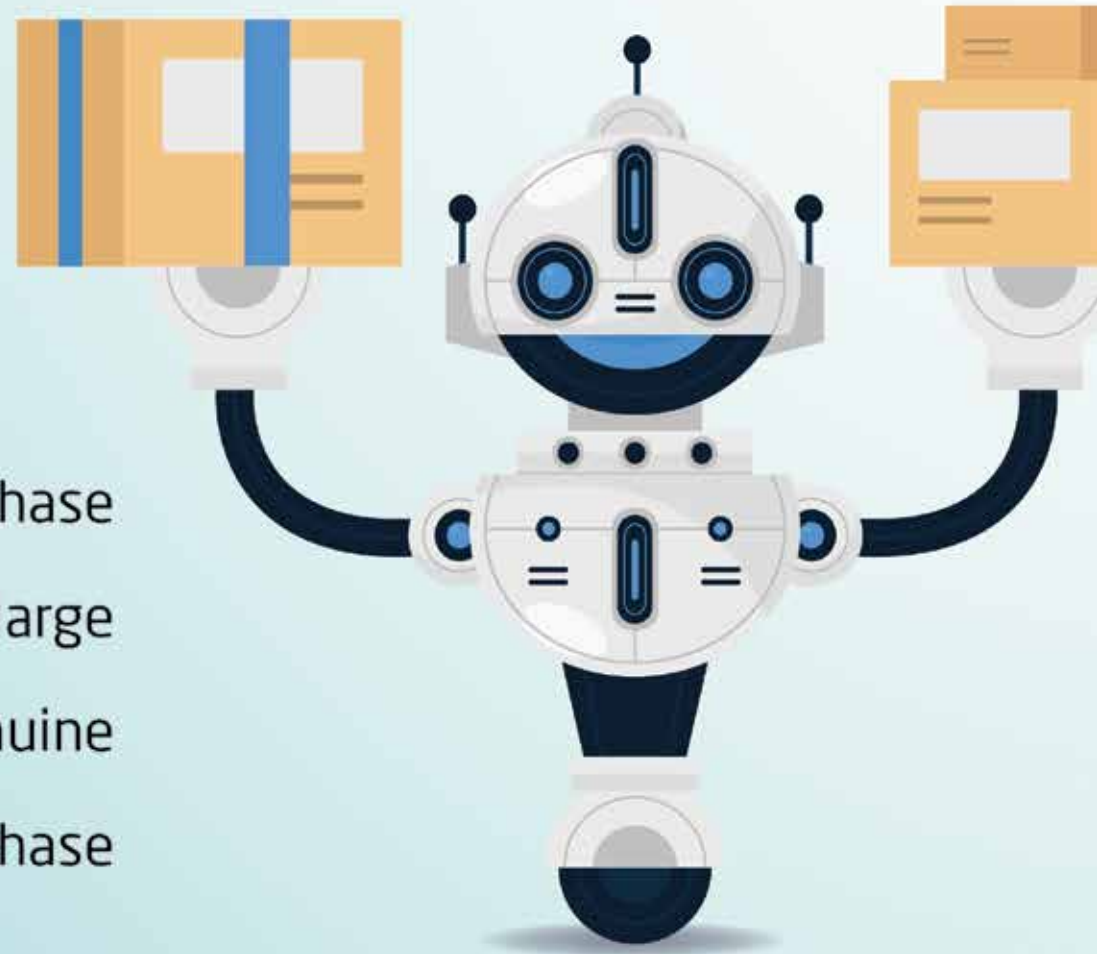
Malicious bots

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.

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.

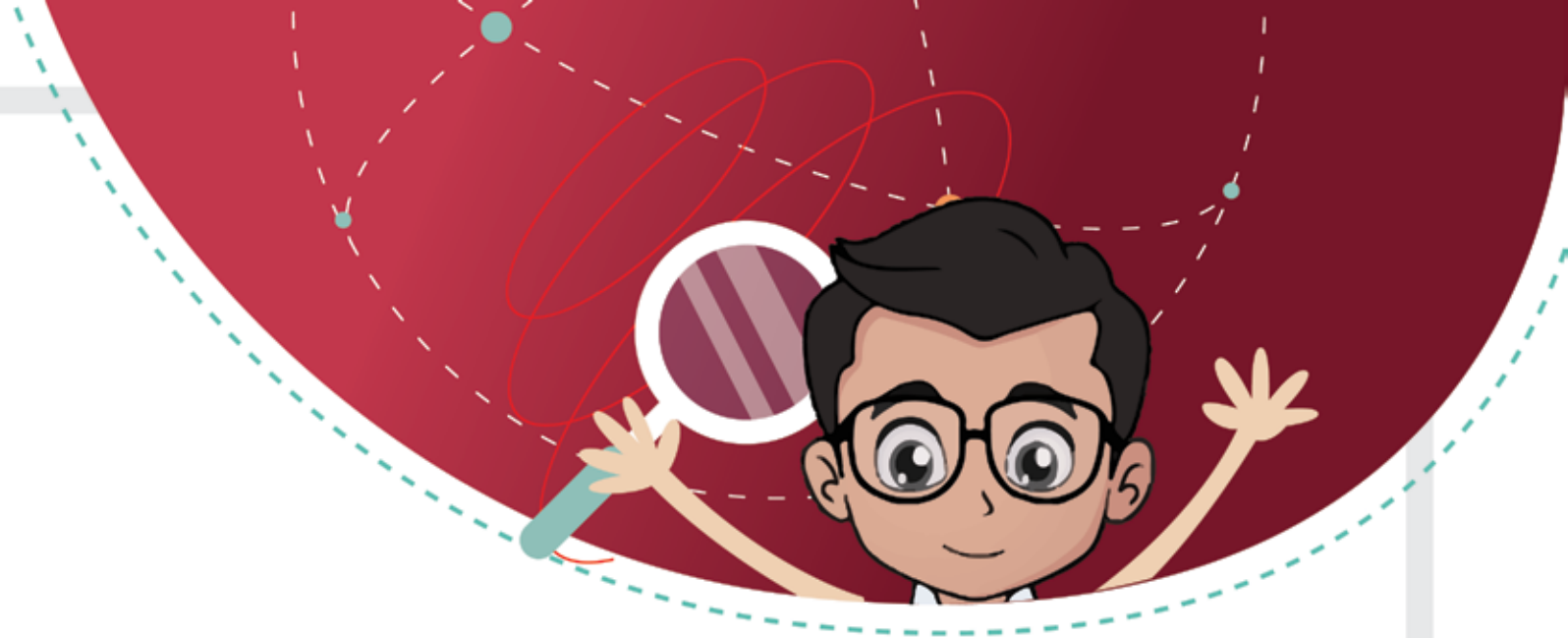


Exercise 2:

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

- A bot is an abbreviation of the word robot, and it is a program that performs tasks (automatically ☒ manually ☐).
- Web bots perform tasks (repeatedly ☒ once only ☐).
- Web bots are considered to be (as fast as humans ☐ faster than humans ☒).
- Web bots can perform tasks that are (useful ☒ unimportant ☐).
- The most important tasks performed by bots are (customer service and search engine indexing ☒ securing personal accounts for users ☐).





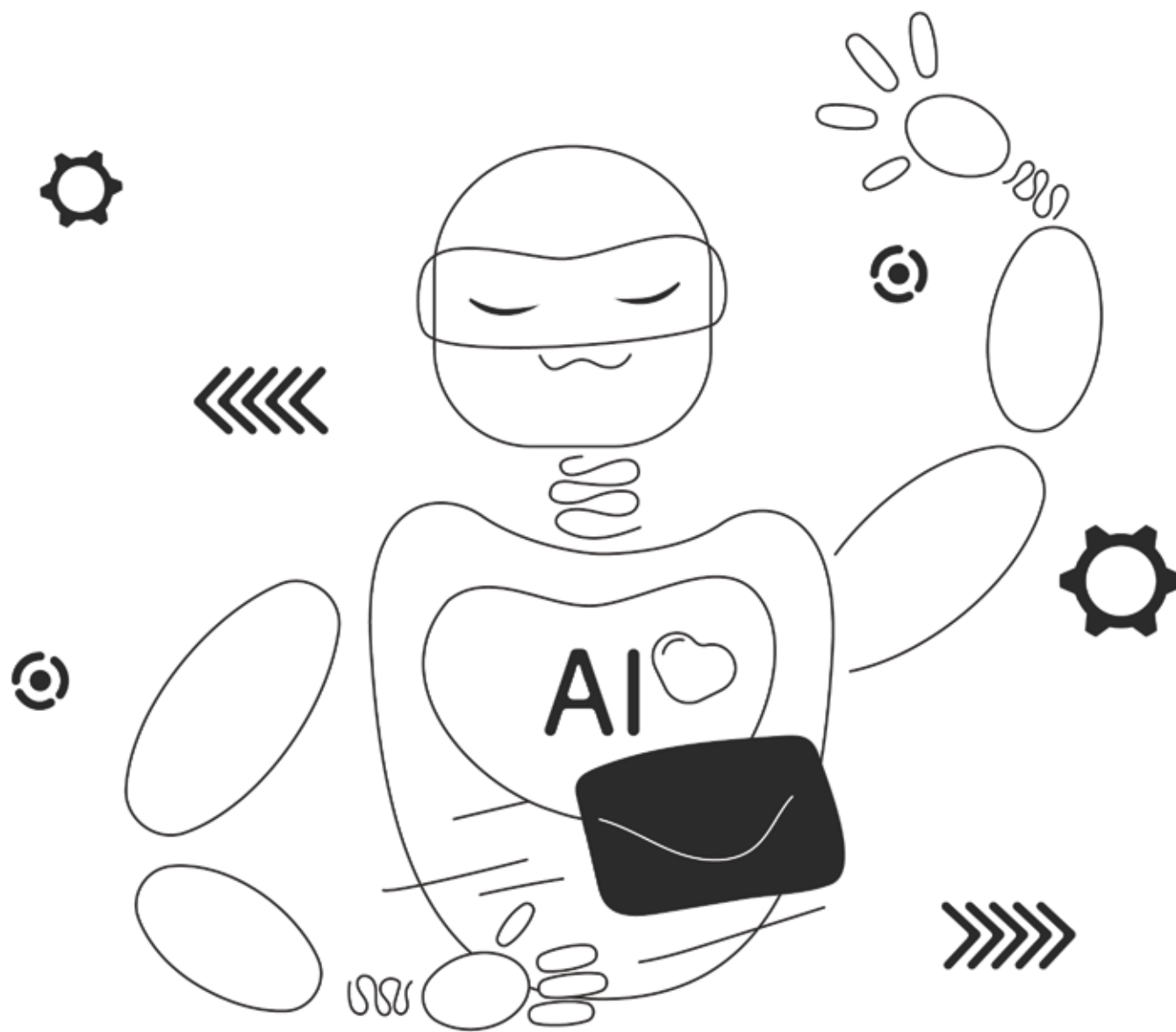
- Web bots can be malware if they (lose control ☐ take full control of the user's computer ☒).
- Computer bots are considered to be (digital tools ☒ security programs ☐.
- Sometimes, bots are misused and exploited to attack (websites ☒ personal accounts ☐.
- Web bots can (mimic ☒ control ☐ human behavior.
- Malicious bots can (promote ☐ disrupt ☒ businesses and attack websites.

Pay attention!

Downloads

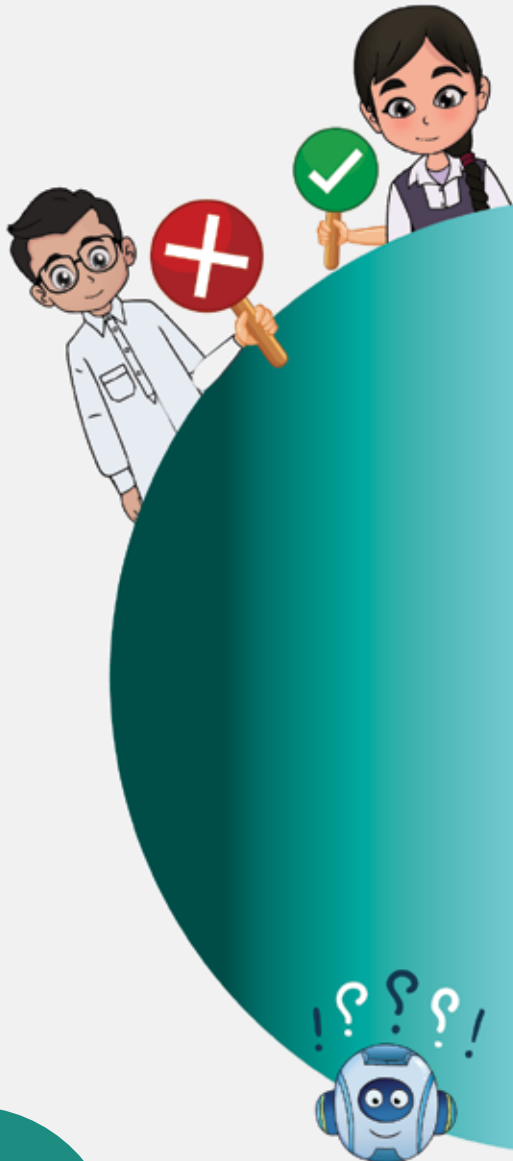
One of the most common ways that bots infect a user's computer, phone and table. This is done by receiving malware in download format through social media or email messages that advise you to click on a link. The link is often in the form of an image or video, and contains either viruses or other malware.





Exercise 3:

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



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.

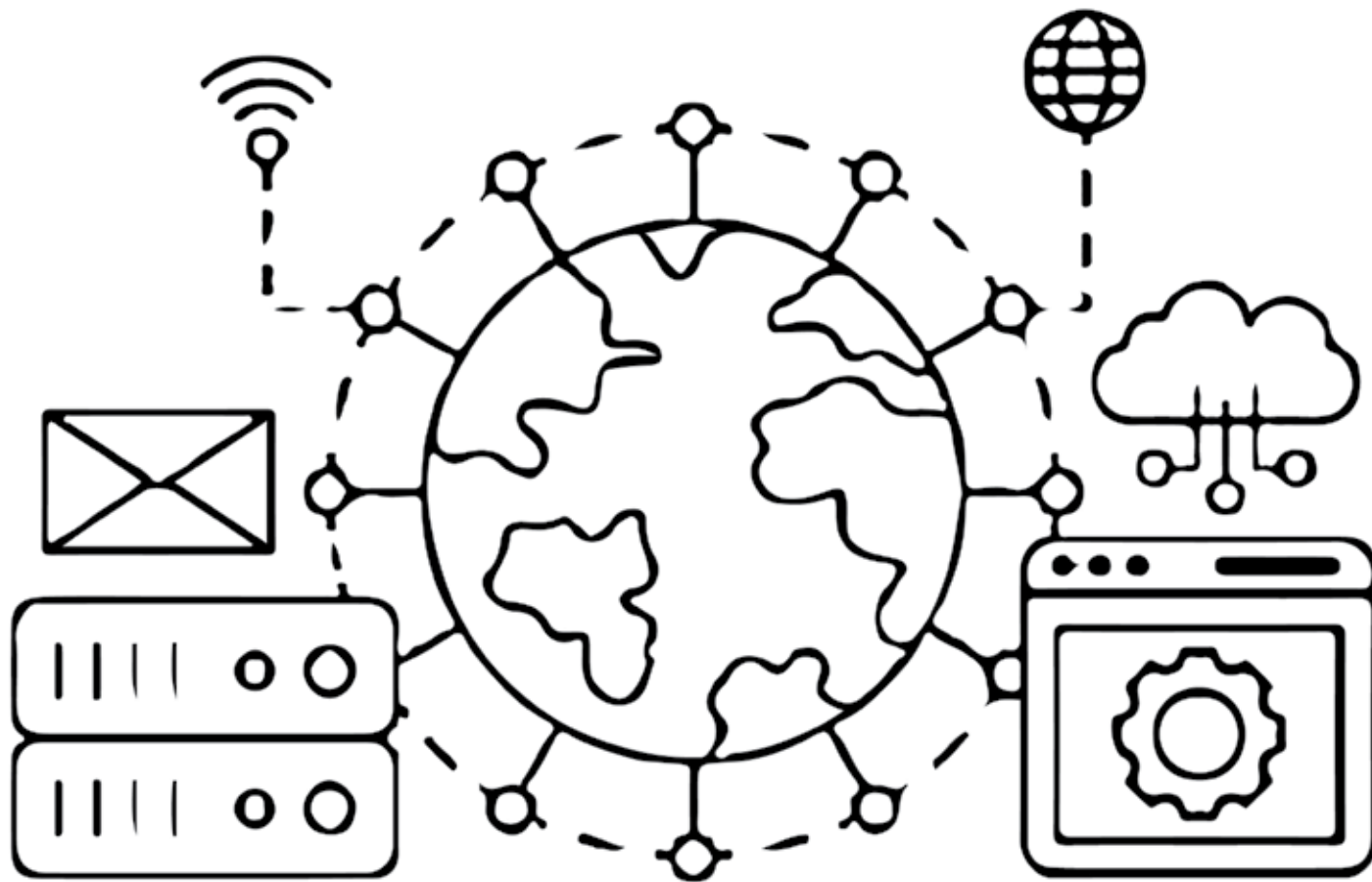




Pay attention!

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:

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.	Social media bots
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.	E-commerce bots
4	These are bots capable of examining the content available on the internet and assisting in handling user queries and responding to their inquiries.	Web crawlers
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.	Web scraping



6	These are bots specialized in gathering information for users by automatically visiting websites to retrieve information and respond to specific questions.	Chatbots
7	These are bots used to monitor the status of websites or systems and assist in providing real-time information.	Task bots
8	These are bots used to complete transactions on behalf of users, allowing users to conduct transactions within the context of the conversation.	Transaction bots
9	These are bots used to automatically download programs or applications from specialized app stores.	Download bots
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.	Ticket Bots



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.	Beneficial bots.
• Chatting to deceive people.	Malicious bots.
• File-sharing bots.	Beneficial bots.
• Ticket bots.	Beneficial bots.
• Monitoring bots.	Beneficial bots.
• Transaction bots,	Beneficial bots.
• Entering credentials.	Beneficial bots.
• DDoS attacks.	Malicious bots.
• Download bots.	Beneficial bots.
• Web scraping crawling bots.	Malicious bots.

- Automated conversation response bot.

Beneficial bots.

- Denial of Inventory Attacks.

Malicious bots.

- Information Gatherers.

Malicious bots.

- Vulnerability scanners.

Beneficial bots.

- Store bots.

Beneficial bots.

- Click Fraud bots.

Malicious bots.

- Activity monitoring.

Beneficial bots.

- Social bots.

Beneficial 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:

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.

~~Algorithms are an essential part of bots and do have significant importance.~~

Chatbots operate automatically without specific pre-defined commands.

~~Chatbots operate automatically within predefined commands.~~

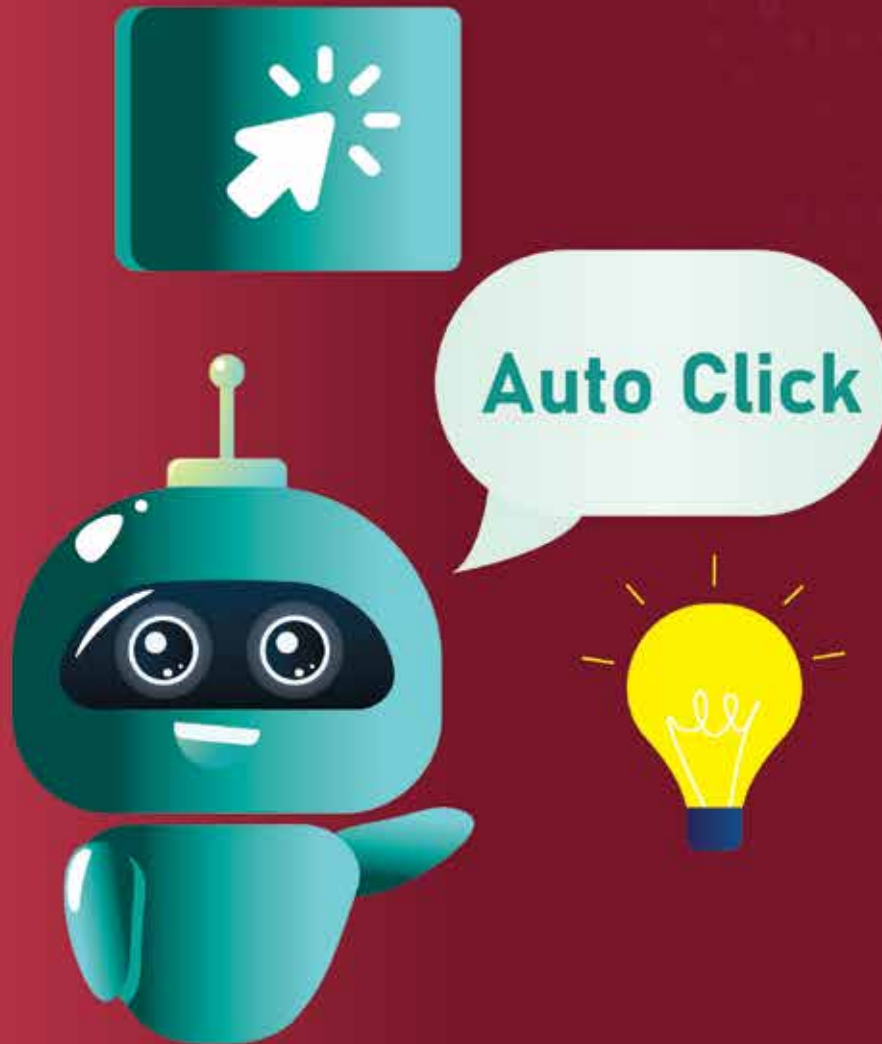
Bots cannot learn from humans.

~~Bots can learn from humans.~~

Bots do not use artificial intelligence technologies.

~~Bots do use artificial intelligence technologies.~~





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:

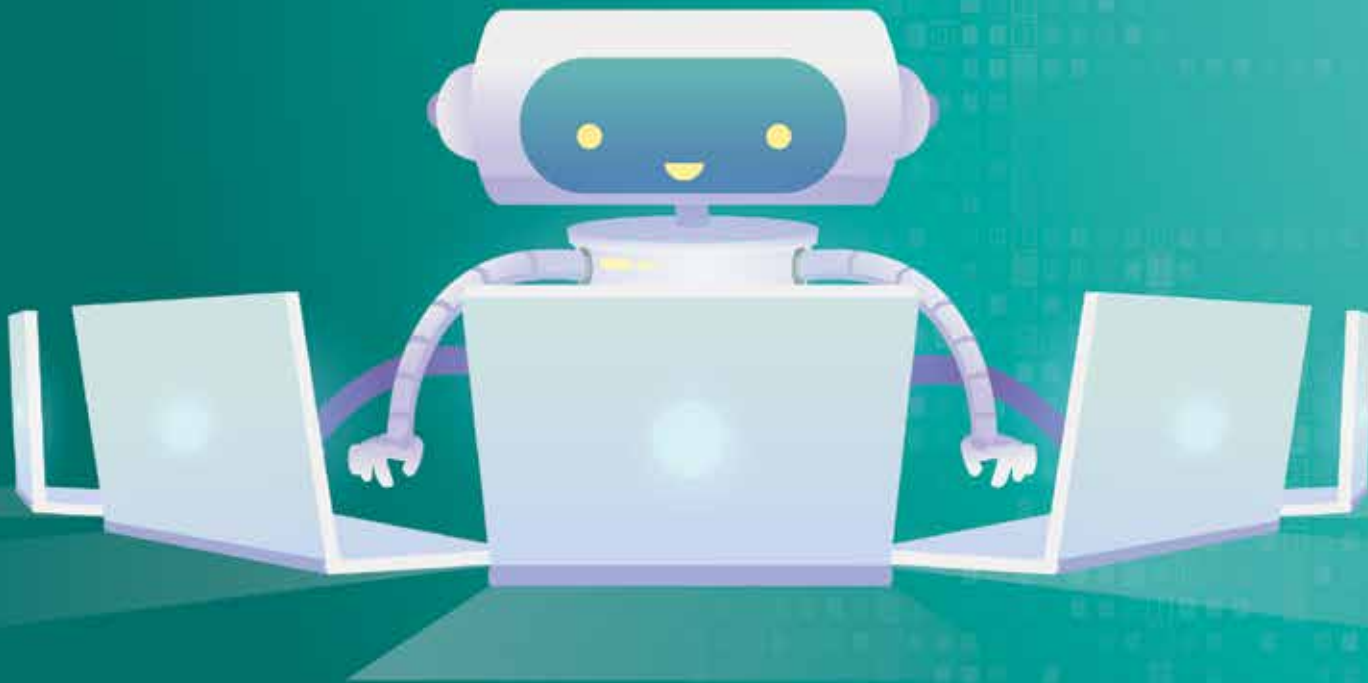
Classify the following sentences as either malicious or beneficial of bots:

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

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:



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



Exercise 3:

Mark (✓) or (✗) in front of the following phrases, correcting them if they are false:

1

You cannot, under any circumstances, fully protect your device from bot attacks.

You can protect your device from bot attacks.



2

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



3

Neglecting software updates has no impact whatsoever.

Failure to install software updates can compromise your data security.



4

Using strong passwords can help to prevent many security problems.



5

You can click on links on the internet without fear.

Clicking on any link on the internet can put your device and data at risk.



6

There are no unreliable websites or ads.

There are unreliable websites and ads.



7

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



8

Using a bot manager does not affect malicious bots.

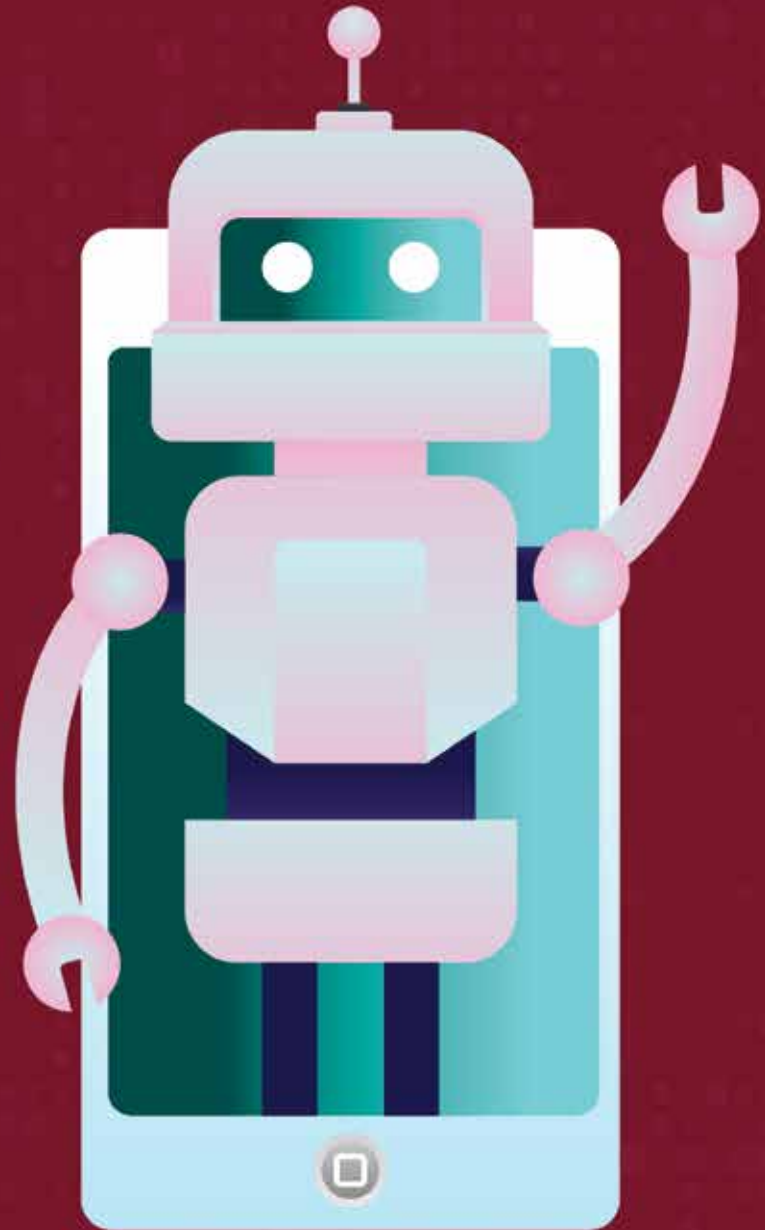
Using a bot manager can help protect against malicious bots.



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.



Did you know that...?

"web crawling programs" bots are used to crawl the internet and find information needed by the users.



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.



Exercise 4:

Extract the
following words
from 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 - engine - Companies - Individuals

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.



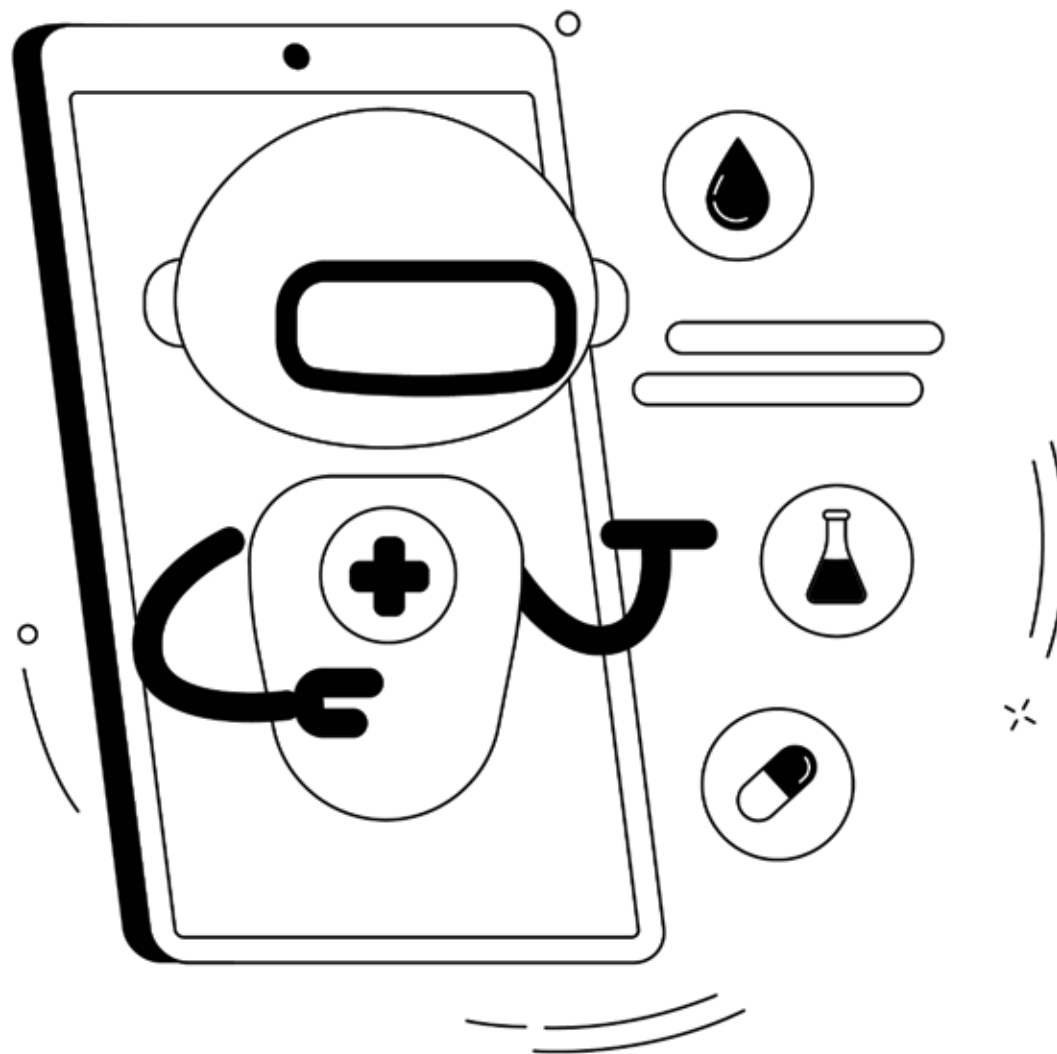
Pay attention!

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!

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.



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!

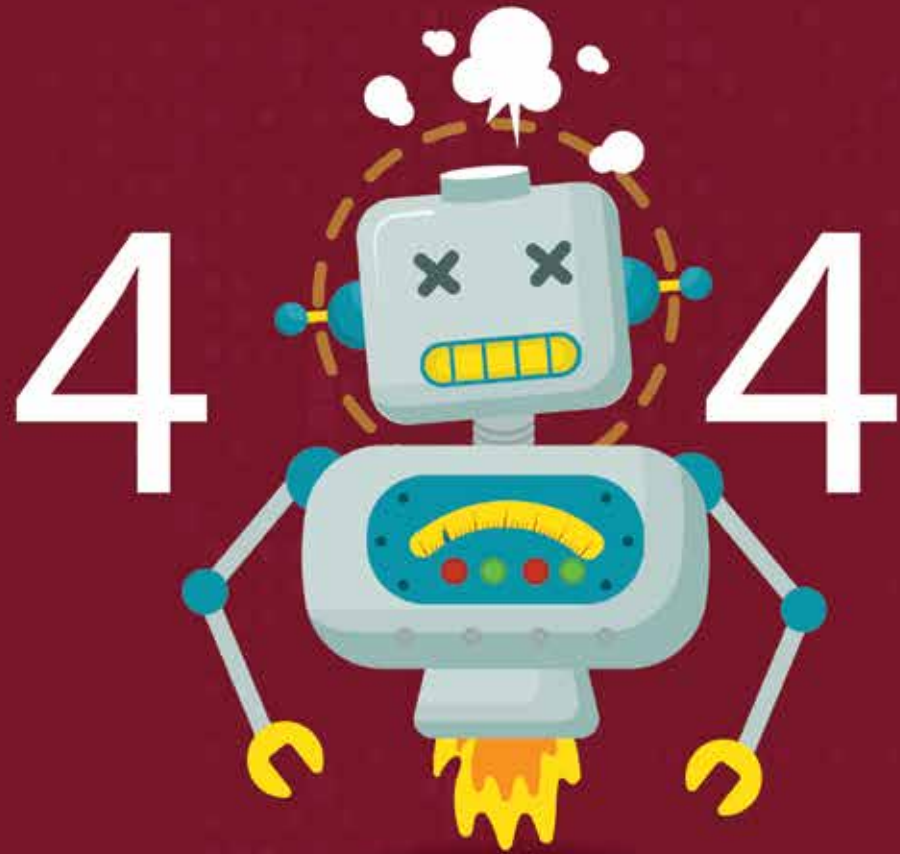
Account takeover (ATO) bots

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



Risks of malicious bots

- Diminution of trust.
- Fraud and theft.
- Manipulation of content.
- DDoS attacks.
- Violations of data privacy.



Features of bots in the Digital Ecosystem

1

Efficiency.

3

Personalization.

2

Availability.

4

Low cost.

5

Scalability.



The benefits of social media bots

1

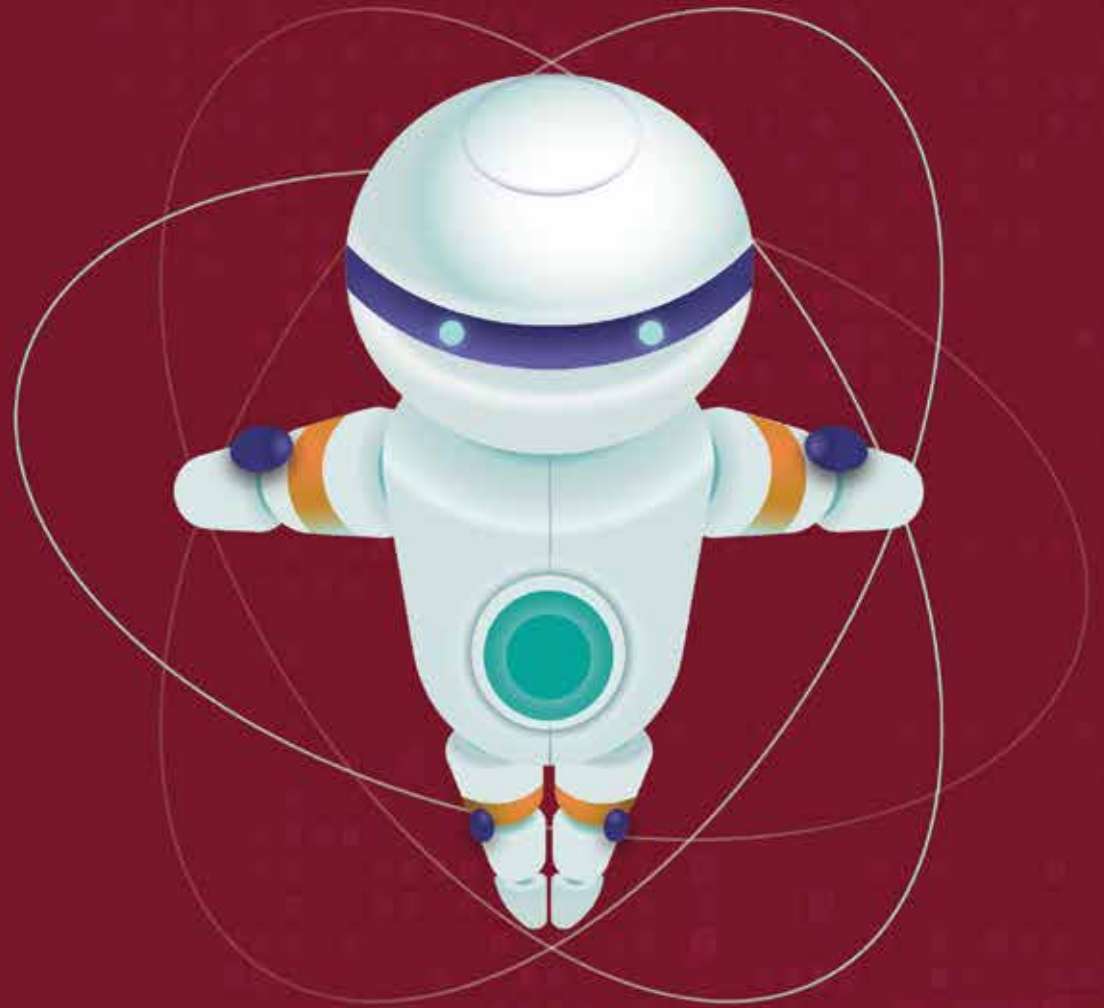
Creating and publishing social media posts.

2

Collecting user information.

3

Providing customer support.



Indications of devices and files being affected by the botnet

- Slow internet speed.
- Decreased processing speed.
- Frequent application crashes.
- Existence of unfamiliar files and applications.
- Increase in the number of unauthorized social media posts and unauthorized email messages.



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

1. Disconnect your device from the Internet.
2. Remove the malware automatically or manually.
3. Report the infection of the bots to the relevant authority.
4. Reset your device and reinstall your operating system.
5. Identify malware using antivirus software.



How to prevent bot Attacks

- Activate the firewall on your device.
- Avoid clicking on suspicious links.
- Install antivirus software.
- Do not download software or programs from unverified sources.
- Regularly update the operating system and other software.
- Set up a guest network on your Wi-Fi router.
- Avoid downloading any email attachments from unfamiliar senders.
- Regularly update the operating system and other software.
- Install antivirus software.





What is it?

A program that performs automated, repetitive, and predetermined tasks. Bots typically mimic or replace human user behavior, but they operate much faster than humans. **The answer: 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. So, it is difficult to determine the source of its traffic.


The answer: Malicious bots

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).

The answer: Chatbots

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

The answer: Task automation bots



It can send unwanted messages to targets, such as spamming software that orchestrate 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.

The answer: Spam Bots

A type of bots that distribute malicious software, such as Ransomware, viruses, Trojans, worms.

The answer: Malware distribution bots

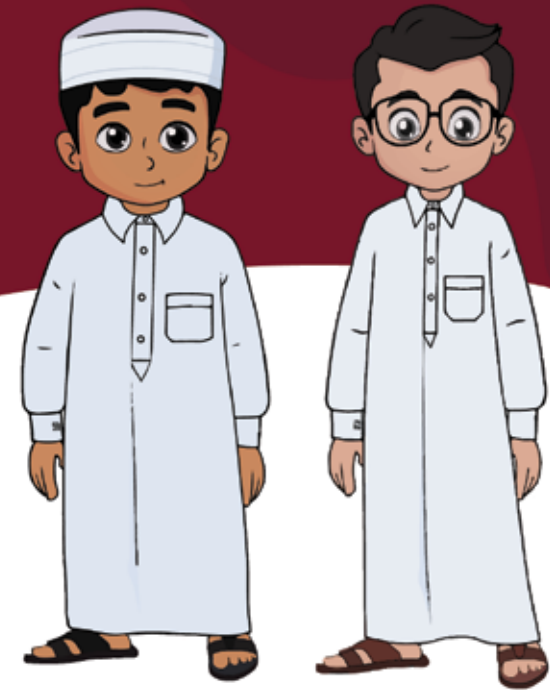
It is a file located on a web server that outlines rules for bot access to the properties on that server.

The answer: Robots.txt

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.

The answer: Bot management

Choose the correct answer:



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

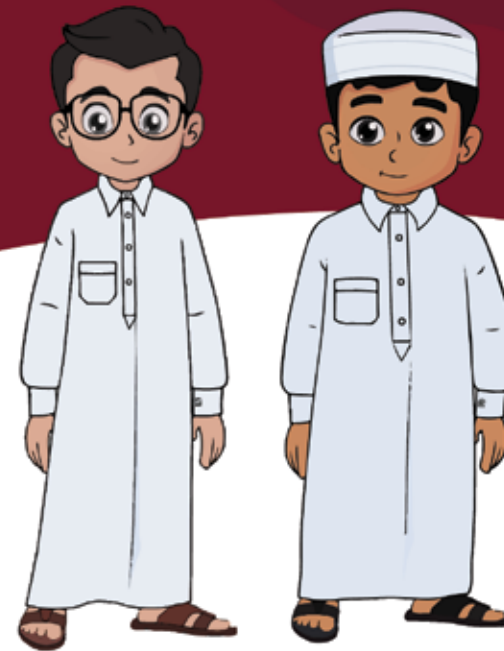
- ☐ Spiders
- ☐ Crawlers
- ☐ Web bots
- ☒ All of the above

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

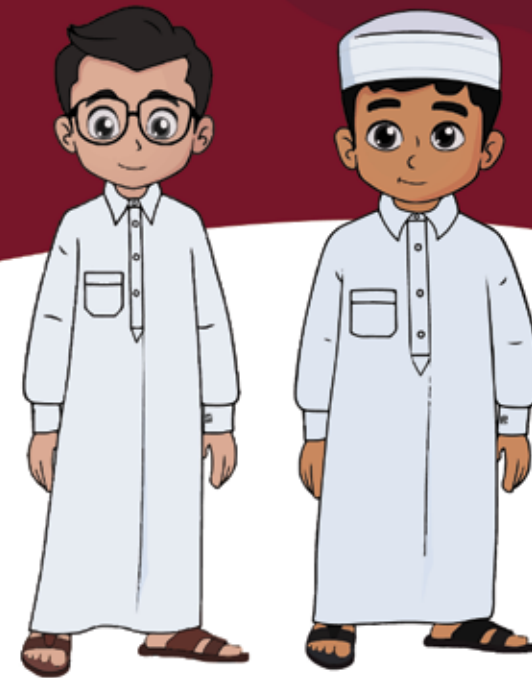
- ☒ Analyzing the behavior of the bot
- ☐ Adding malicious bot programs to the allowed lists
- ☐ Not limiting the excessive use of bots for service
- ☐ Allowing malicious bots access to specific content

8- A type of automated chatbot software that provides product recommendations and assists in purchasing products

- ☒ E-commerce bots
- ☐ Social media bots
- ☐ Chatbots

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.

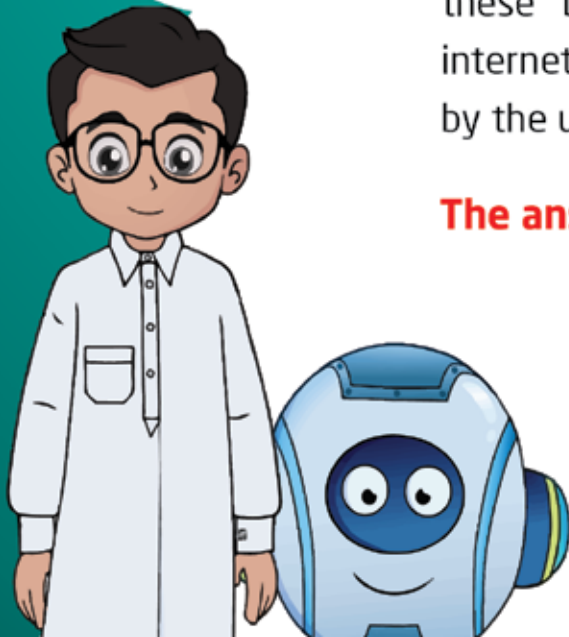
The answer: Web bots.

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.

The answer: Search engine bots.

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.

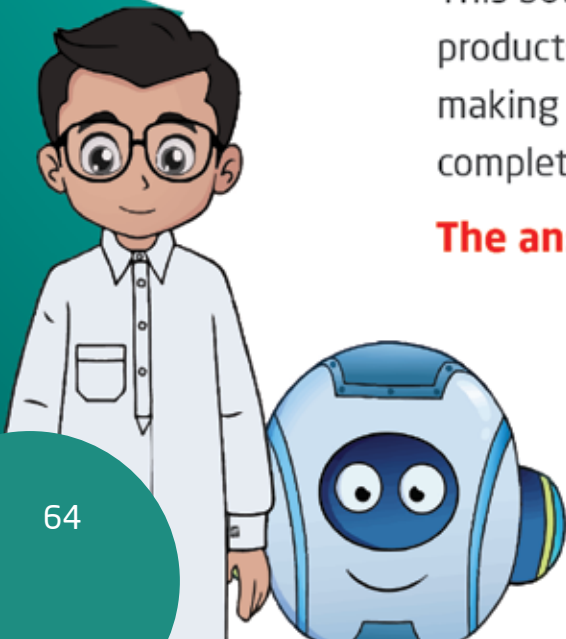
The answer: Web bots.

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.

The answer: Exploitative bots

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.

The answer: Data collectors

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



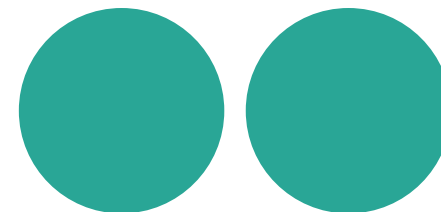
Graduation Project

The graduation project is an assignment that you undertake on your own or in collaboration with one or two of your colleagues, under the supervision of the trainer. Through it, you are required to perform one of the following assignments:

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



References



1. A Chronological Look at the Biggest Botnet Attacks of the 21st Century. On site: <https://cutt.us/VjYSb>
2. Advantages of Robots in the Workplace, robotics tomorrow. On site: <https://cutt.us/ph64H>
3. Glupteba Botnet Continues to Thrive Despite Google's Attempts to Disrupt It. On site: <https://cutt.us/yKrWy>
4. How is an Internet bot constructed? Cloudflare. On site: <https://cutt.us/XtS2O>
5. How to Block Bad Bots on Your Website - 4 Mitigation Methods. On site: <https://cutt.us/XINPY>
6. Microsoft Hijacks Necurs Botnet that Infected 9 Million PCs Worldwide. On site: <https://cutt.us/ecKXV>
7. Rizwan Ur Rahman & Deepak Singh Tomar. New biostatistics features for detecting web bot activity on web applications, , 2020, on site: <https://cutt.us/MtBbH>
8. Types of Bots: An In-Depth Guide by Radware, radware. On site: <https://cutt.us/Wee8j>
9. What is a Botnet and How to Protect Your Devices in 2023? On site: <https://cutt.us/Xh56M>
10. What is a Botnet and How to Protect Your Devices in 2023? On site: <https://cutt.us/Xh56M>
11. What is a brute force attack? On site: <https://cutt.us/YYbNT>
12. What is a DDoS attack? On site: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>
13. What is a web crawler bot? Cloudflare. On site: <https://cutt.us/SWZvK>
14. What is bot management? | How bot managers work, Cloudflare. On site: <https://cutt.us/5cnit>
15. What is click fraud? On site: <https://cutt.us/zD5On>
16. What is click fraud? On site: <https://cutt.us/zD5On>
17. What is content scraping? | Web scraping. On site: <https://cutt.us/N1xas>
18. What is credential stuffing? | Credential stuffing vs. brute force attacks, Cloudflare. On site: <https://cutt.us/GpCSq>
19. What is the Mirai Botnet? On site: <https://cutt.us/mrCRO>
20. Types of bots. An In-Depth Guide by Redware. On site: <https://cutt.us/dN7Wo>
21. Shanika Wickramasinghe. Bot Types 101: Bad Bots, Good Bots and Everything in Between, July, 2023. On site: <https://cutt.us/i3NJc>
22. What are bots? - Definition and Explanation, Kaspersky, on site: <https://cutt.us/eX64R>





CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency