روبوتات الشَّبَكة العَالَميَّة

شرائح العَرْض

حقيبة خاصّة بالمُدَرِّب

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المرحلة الثَّانويَّة

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

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

فهرس المحتوى العِلْمِيّ

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تمهيد	5 دقائق
الجُزْء النَّظريّ من المادَّة	25 دقيقة
عَرْض الفيديوهات التَّعليميَّة	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الألْعَاب التَّدريبيَّة	25 دقيقة
حِوَار ونِقَاش مع الطَّلَبة	15 دقيقة
مَشروع التَّخرُّج	5 دقائق
المُدَّة الزَّمنيَّة للورشَة	ساعتان

الفَصْل الأوَّل
مفهوم روبوتات الشَّبكة العالميَّة وأنواعها

مفهوم روبوتات الشّبكة العالميّة

الرُّوبوت

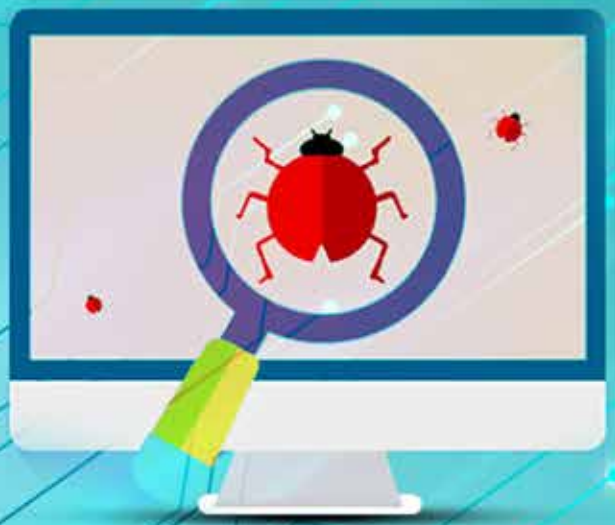
هو برنامج يُنفِّذ مهامّ تلقائيَّة ومُتكرِّرة ومحدَّدة مسبقًا، وعادةً ما تُقلِّد الرُّوبوتات سلوك المُستخدِم البشريّ أو تحلّ محلّه، لكنَّها تعمل بشَكْلٍ أسرع بكثير من المُستخدِمين البشر، وتؤدِّي الرُّوبوتات وظائف مفيدة، مثل خدمة العملاء أو فهرسة محرِّكات البحث، ولكنَّها يمكن أن تأتي أيضًا في شكل برمجيات ضارَّة تُستخدَم للتَّحكُّم الكامل في جهاز الحاسوب.

ويُطلَق على روبوتات الإنترنت مسمَّيات أخرى مثل: العناكب أو برامج الزَّحف أو روبوتات الويب.

تعريف الرُّوبوتات الضَّارَّة

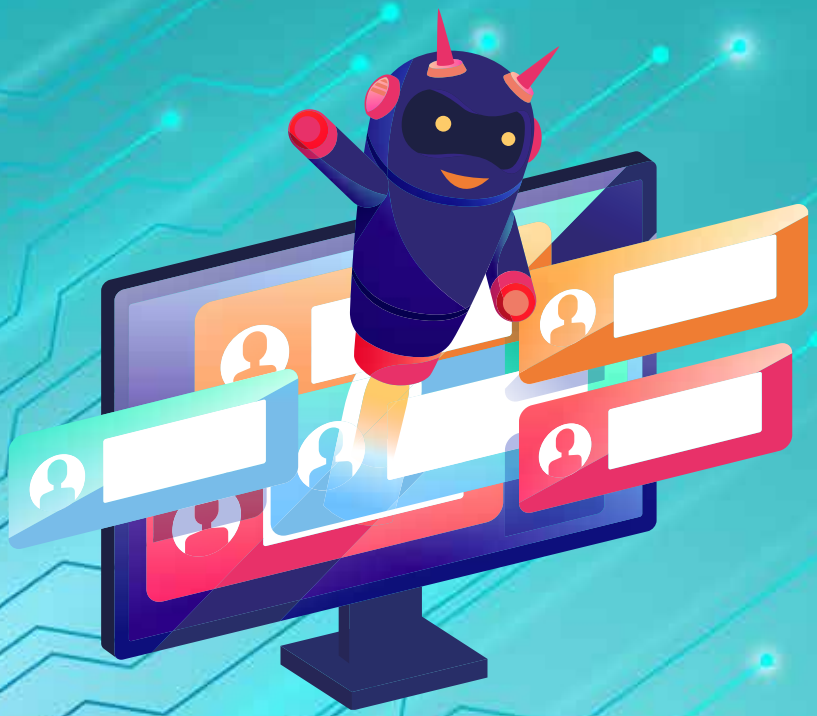
عبارة عن عدد من الأجهزة المتَّصلة بالإنترنت، يعمل كلّ منها على تشغيل روبوت واحد أو أكثر، وذلك غالبًا دون عِلْم مالِكِي الأجهزة، ولأنّ كلّ جهاز له عنوان IP خاصّ به، فإنّ حركة مرور شبكة الرُّوبوتات تأتي من عناوين IP متعدِّدة؛ لذا يَصْعُب تحديد مصدر حركة مرور الرُّوبوت الضَّارّ وحظره.

ويمكن لشبكات الرُّوبوتات تطوير نفسها باستخدام أجهزة لإرسال رسائل بريد إلكترونيّ غير مرغوب فيها، التي يمكن أن تُصيب مزيدًا من الأجهزة.



مهمَّة الرُّوبوتات الضَّارَّة

يمكن برمجة الرُّوبوتات الضَّارَّة وروبوتات الإنترنت لاقتحام حسابات المُستخدِمين، أو فحص الإنترنت؛ بحثًا عن معلومات الاتِّصال، أو إرسال رسائل غير مرغوب فيها، أو القيام بأعمال ضارَّة أخرى؛ حيث يقوم المُهاجِمون بتوزيع الرُّوبوتات السَّيِّئة في شبكة الرُّوبوتات لتنفيذ هذه الهجمات وإخفاء مصدر حركة مرور الهجوم.



أنواع روبوتات الشَّبكة العالميّة

الرُّوبوتات

هي تطبيقات برمجيَّة مُصمَّمة لأتمتة مهامّ محدَّدة وللتَّفاعُل مع المُستخدِمين، وغالبًا ما تُحاكي المحادثة البشريَّة في حالة روبوتات الدَّردشة، وهي مبرمَجة لاتِّباع قواعد محدَّدة مسبقًا أو لاستخدام خوارزميَّات الذَّكاء الاصطناعيّ (AI) لمعالجة اللُّغة الطَّبيعيَّة وتقديم الاستجابات.

أهمِّيَّة الرُّوبوتات

الكفاءة

إذ يمكن للرُّوبوتات التَّعامل مع المهامّ المُتكرِّرة والعاديَّة بشَكْلٍ أسرع بكثير من البشر، ممَّا يزيد من الكفاءة والإنتاجيَّة بشَكْلٍ عامّ.

إضفاء الطَّابع الشَّخصيّ

يمكن للرُّوبوتات المُتقدِّمة ذات قدرات الذَّكاء الاصطناعيّ أن تتعلَّم من تفاعلات المُستخدِم، ممَّا يُوفِّر تجارب مخصَّصة مع مرور الوقت.

التَّوفُّر

يمكن أن تعمل الرُّوبوتات على مدار السَّاعة طوال أيَّام الأسبوع، ممَّا يُوفِّر مساعدة فوريَّة للمُستخدِمين دون الحاجة إلى تدخُّل بشريّ.

انخفاض التَّكلِفة

من خلال القيام بالمهامّ، يمكن للرُّوبوتات أن تُساعِد في تقليل تكاليف العِمَالة وتحسين تخصيص الموارد.

قابليَّة التَّوسُّع

تتعامل الرُّوبوتات مع تفاعلات متعدِّدة في وقت واحد، ممَّا يجعلها مثاليَّة للتَّعامل مع كمِّيَّات كبيرة من الاستعلامات أو المعاملات.

تنقسم الرُّوبوتات بشَكْلٍ عامّ إلى نوعين رئيسين

01 Chatbots

وقد صُمِّمت للمشاركة في المحادثات مع المُستخدِمين، وذلك عادةً من خلال واجهات نصِّيَّة أو صوتيَّة.

02 روبوتات أتمتة المهــامّ

هذا النَّوع من الرُّوبوتات يُركِّز على أتمتة المهامّ شائعة الاستخدام ومعالجة البيانات، وغيرها من الأنشطة التي قد تستغرق وقتًا طويلًا من البشر.

ما الرُّوبوتات الجيِّدة؟

الرُّوبوتات الجيِّدة هي روبوتات مُصمَّمة لأداء أنشطة مشروعة، بخلاف الرُّوبوتات الضَّارَّة، ولها عدَّة أنواع هي:

01

روبوتات محرِّك البحث

تُعرف أيضًا باسم "برامج زحف الويب".

02

روبوتات مدقِّق الرَّوابط الخلفيَّة

تُعْتبر الرَّوابط الخلفيَّة مهمَّة في تحسين محرِّكات البحث (SEO)، وتُساعِد الرُّوبوتات على اكتشاف الرَّوابط الخلفيَّة لصفحة ويب معيَّنة وتحليل تَقَدُّمها وجودتها.

03

روبوتات وسائل التَّواصل الاجتماعيّ

صُمِّمت هذه الرُّوبوتات لأتمتة المهامّ على منصَّات التَّواصل الاجتماعيّ.

04

روبوتات الدَّردشة

الهدف الرَّئيس لها هو تقديم المساعدة للعملاء على مدار السَّاعة طوال أيَّام الأسبوع.

05

روبوتات الألعاب

صُمِّمت خصوصًا لأداء الأنشطة المتعلِّقة بالألعاب، مثل محاكاة اللَّاعبين الحقيقيِّين في الألعاب.

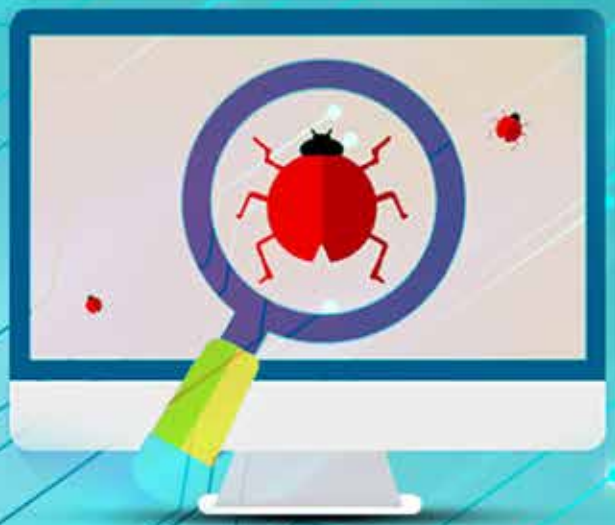
06

روبوتات التِّجارة الإلكترونيَّة

تُوفِّر التَّوصية بالمنتجات وتُساعِد في شراء المنتجات.

الرُّوبوتات الضَّارَّة

هي روبوتات مُصمَّمة للقيام بأنشطة ضارَّة مختلفة، فهي تستغلّ نقاط الضَّعف للوصول غير المُصرَّح به إلى حسابات المُستخدِمين، كما يمكن للرُّوبوتات الضَّارَّة استهداف مؤسَّسات معيَّنة لتشويه صورتها على وسائل التَّواصل الاجتماعيّ من خلال نَشْر أخبار مزيَّفة أو إرسال بريد عشوائيّ إلى كلّ شخص يعرفونه.



أنواع الرُّوبوتات الضَّارَّة

01 روبوتات DDoS

صُمِّمت لشنّ هجمات حجب الخدمة الموزَّعة (DDoS) على مواقع الويب أو الشَّبكات أو الخوادم.

02 روبوتات Spam

يمكن لروبوتات Spam إرسال رسائل غير مرغوب فيها إلى الأهداف، مثل شنّ هجمات تصيُّد أو نَشْر تعليقات سيِّئة على وسائل التَّواصل الاجتماعيّ لتشويه صورة علامة تجاريَّة أو شركة معيَّنة، وكذلك تسويق منتجات أو خدمات غير قانونيَّة.

أنواع الرُّوبوتات الضَّارَّة

03 روبوتات الاستيلاء على الحساب (ATO)

تُعْرف أيضًا باسم "روبوتات حَشْو بيانات الاعتماد"، وتستطيع الوصول إلى حسابات المُستخدِمين عن طريق استخدام أسماء المُستخدِمين وكلمات المرور المسروقة.

04 روبوتات توزيع البرمجيات الضَّارَّة

يمكن لهذه الرُّوبوتات توزيع البرمجيات الضَّارَّة مثل برمجيات الفدية والفيروسات وأحصنة طروادة وديدان الحاسوب وغيرها، من خلال استغلال نقاط الضَّعف في الأنظمة المُستهدَفة ونَشْر البرمجيات الضَّارَّة.

أنواع الرُّوبوتات الضَّارَّة

05 روبوتات المستغلّ

هي روبوتات مُصمَّمة لشراء منتجات أو خدمات سريعة الحركة بكمِّيَّات كبيرة.

06 روبوتات النَّقــر

تعمل على خداع المعلنين من خلال نقرات المُستخدِم المُصْطَنعة، فهي تخدع تصنيفات محرِّك البحث.

مخاطر الرُّوبوتات الضَّارَّة

التَّلاعب بالمحتوى

إذ تؤدِّي إلى انتشار المعلومات الخاطئة، أو خَلْق تصوُّرٍ منحرفٍ للرَّأي العامّ.

انتهاكات خصوصيَّة البيانات

قد تستغلّ الرُّوبوتات نقاط الضَّعف في الأنظمة للوصول غير المُصرَّح به إلى بيانات المُستخدِم الحسَّاسة، ممَّا يؤدِّي إلى انتهاكات الخصوصيَّة وسرقة الهُويَّة.

هجمات حجب الخدمة الموزَّعة (DDoS)

تُستخدَم شبكات الرُّوبوتات -وهي شبكات من أجهزة الحاسوب المخترقة التي يتحكَّم فيها كيان واحد- لشنّ الهجمات ضدّ الخوادم وتعطيل الخدمات.

تَراجُـــع الثِّقـــة

تؤدِّي هجمات الرُّوبوتات الضَّارَّة إلى انخفاض ثقة المُستخدِمين في المنصَّات والشَّركات عبر الإنترنت.

الاحتيال والسَّرقة

يمكن استخدامها لتنفيذ أنشطة احتياليَّة مثل الاستيلاء على الحساب، أو سرقة معلومات التَّعريف الشَّخصيَّة أو نَشْر معلومات مُضلِّلة.

روبوتات الويب النّافعة والضّارّة

الرُّوبوتات النَّافعة

تلعب هذه الرُّوبوتات دورًا أساسيًّا في عمل النِّظام البيئيّ للويب، وهي برامج آليَّة مُصمَّمة لأداء مهامّ محدَّدة تُفيد المُستخدِمين وأصحاب مواقع الويب، فهي تَخدِم أغراضًا مشروعة، مثل فهرسة محتوى الويب، وتحسين رؤية محرِّك البحث، وجَمْع البيانات للأدلَّة، وتحسين تجربة المُستخدِم.

أنواع الرُّوبوتات النَّافعة

01 عناكب الويب (برامج زحف الويب)

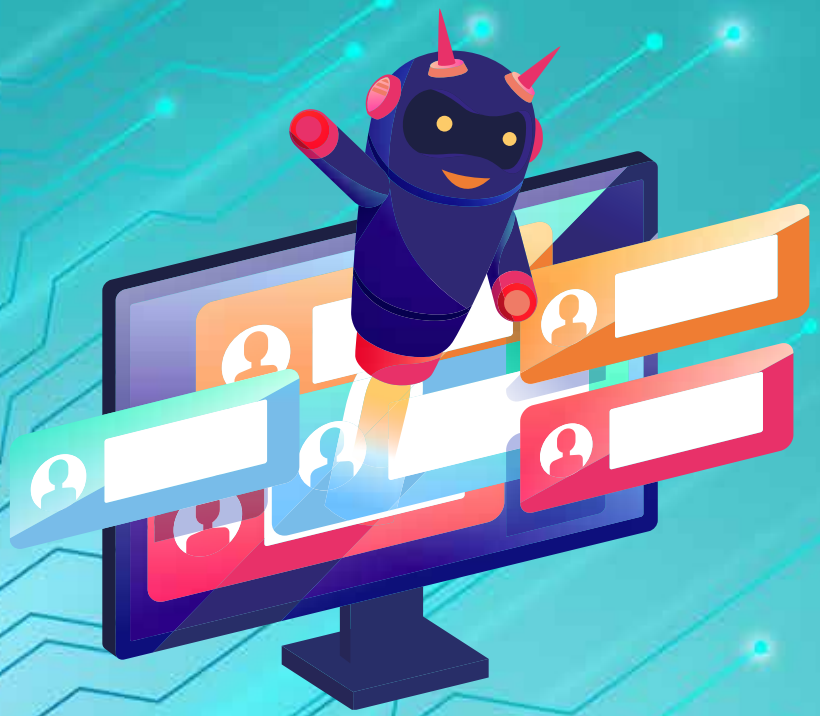
تقوم هذه الرُّوبوتات بالزَّحف إلى مواقع الويب وجَمْع المعلومات وفهرستها في قاعدة بيانات محرِّك البحث.

02 مُجَمِّعُو البيانـات

هي روبوتات مُصمَّمة لجَمْع المعلومات من مصادر مختلفة وإنشاء أدلَّة شاملة أو قوائم محتوى؛ حيث تقوم هذه الرُّوبوتات بجَمْع البيانات وتحديثها لتزويد المُستخدِمين بمعلومات مُحَدَّثة بشأن مواقع الويب أو الشَّركات أو المنتجات أو الخدمات.

ما هجوم الرُّوبوت؟

هو نوع من الهجمات الإلكترونيَّة التي تستخدم البرمجيات النَّصِّيَّة الآليَّة لتعطيل الموقع أو سرقة البيانات أو إجراء عمليَّات شراء احتياليَّة أو تنفيذ إجراءات ضارَّة أخرى، ويمكن نَشْر هذه الهجمات ضدّ العديد من الأهداف المختلفة، مثل مواقع الويب والخوادم والتَّطبيقات، ويختلف غرض هذه الهجمات، لكنَّها غالبًا ما تتضمَّن سرقة معلومات حسَّاسة أو تتسبَّب في تلف البنية التَّحتيَّة للهدف.



أنواع هجوم الرُّوبوتات الضَّارَّة

01 حَشْو بيانات الاعتماد Credential Stuffing

هو هجوم إلكترونيّ يتمّ فيه استخدام بيانات الاعتماد التي تمّ الحصول عليها من خرق البيانات.

02 سرقة الويب/ المحتوى Web/Content Scraping

تحدث عندما تقوم الرُّوبوتات بتنزيل محتوًى من موقع ويب لاستخدامه في الهجمات المستقبليَّة، ويُرسِل روبوت استخراج المعلومات من موقع الويب سلسلةً من الطَّلبات وينسخ المعلومات ويحفظها، كلّ ذلك في غضون ثوانٍ.

أنواع سرقة الويب/ المحتوى

سرقة الاتّصال

سرقة الأسعار

يحدث هذا عندما تقوم إحدى الشَّركات بتنزيل جميع معلومات التَّسعير من موقع الويب الخاصّ بشركة منافسة؛ حتى تتمكَّن من تعديل أسعارها وفقًا لذلك.

أنواع هجوم الروبوتات الضارة

01 هجوم DDoS

يُعَدّ هجوم حَجْب الخدمة الموزَّع (DDoS) محاولة خبيثة لتعطيل حركة المرور العاديَّة لخادم أو خدمة أو شبكة مُستهدَفة.

02 هجوم القوَّة الغاشمة

هو أسلوب التَّجربة والخطأ المُستخدَم لفكّ تشفير البيانات الحسَّاسة، والتَّطبيقات الأكثر شيوعًا لهجمات القوَّة الغاشمة هي كسر كلمات المرور وتكسير مفاتيح التَّشفير.

طُرق الوقاية من هجمات القوّة الغاشمة

- اختيار كلمات مرور أطول وأكثر تعقيدًا.
- تمكين المصادقة الثُّنائيَّة واستخدام كلمات مرور فريدة لكلّ خدمة.
- تجنُّب إدخال كلمات المرور أو المعلومات الشَّخصيَّة -مثل أرقام بطاقات الائتمان أو المعلومات المصرفيَّة- في أيّ خدمة ويب لا تحمي البيانات بمفاتيح تشفير قويَّة.

أنواع هجوم الرُّوبوتات الضَّارَّة

03 النَّقــر الاحتيـاليّ

يحدث النَّقر الاحتياليّ عندما يتظاهر شخص أو روبوت بأنَّه زائر شرعيّ لصفحة ويب وينقر على إعلان أو زرّ أو أيّ نوع آخر من الارتباطات التَّشعُّبيَّة (القوائم الدَّاخليَّة)، والهدف هو خداع النِّظام الأساسيّ أو الخدمة للاعتقاد أنّ المُستخدِمين الحقيقيِّين يتفاعلون مع صفحة ويب أو إعلان أو تطبيق.

دوافع النَّقر الاحتياليّ

01
يسعى المحتالون إلى تحقيق مكاسب ماليَّة.

02
بالنِّسبة إلى المؤسَّسات، يهدف النَّقر إلى الإضرار بميزانيَّات الإعلانات الخاصَّة بمنافسيها.

03
دوافع أيديولوجيَّة؛ إنّ الإعجابات المُصطنَعة -أو التَّصويت الإيجابيّ لمنشور ما- تهدف إلى جَعْل بعض المشاعر تبدو أكثر شعبيَّة ممَّا هي عليه بالفعل.

04
يمكن لمُجْرمي الإنترنت استخدام النَّقر الاحتياليّ لجَعْل صفحة الويب الضَّارَّة تَظْهَر في مرتبة أعلى في تصنيفات البحث بحيث تبدو شرعيَّة.

الأنواع الشَّائعة من النَّقرات الاحتياليَّة

- الاحْتِيَال في الإعلانات.
- الاحْتِيَال على مواقع الإنترنت.
- هُجوم ماليّ على الشَّركة التي تَدْفَع مقابل الإعلانات.
- التَّلاعُب بتصنيفات محرِّك البحث من خلال زيادة نسبة النَّقر؛ بهدف الظُّهور بشَكْلٍ مُصْطَنع.

ما روبوت النَّقر؟

هو روبوت تمتّ برمجته لتنفيذ النَّقرات الاحتياليَّة، فأبسط روبوتات النَّقر تصل فقط إلى صفحة ويب وتنقر على الرَّابط المطلوب، كما تتمّ برمجة روبوتات النَّقر المُصمَّمة جيِّدًا لاتِّخاذ الإجراءات التي قد يتَّخذها المُستخدِم الحقيقيّ أيضًا، مثل حركات الفأرة (الماوس) والإيقاف المؤقَّت العشوائيّ قبل اتِّخاذ الإجراء.

هل يتمّ النَّقر الاحتياليّ من الرُّوبوتات فقط؟

يمكن تنفيذ النَّقر الاحتياليّ أيضًا بواسطة عُمَّال بشريِّين ذوي أجور منخفضة، ويُطلَق على مجموعة هؤلاء العُمَّال اسم "مزرعة النَّقرات"، وغالبًا ما يتمّ تشغيل مزارع النَّقرات في المناطق التي تكون فيها الأجور رخيصةً نسبيًّا، كما هو الحال في البلدان النَّامية.

حيث يقوم عُمَّال مزرعة النَّقر بالانتقال إلى صفحات ويب معيَّنة والنَّقر على الرَّوابط المخصَّصة؛ لتضخيم معدَّلات النَّقر أو إجماليَّات حركة المرور لتلك الصَّفحات بشَكْلٍ مُصْطَنع، ويمكنهم أيضًا أن يكونوا نشطين على شبكات التَّواصل الاجتماعيّ وأن "يُسجِّلوا إعجابهم" بمنشورات أو صفحات معيَّنة لتعزيز ظهورهم.

الفَصْل الثَّاني
آليَّة عمل روبوتات الشَّبكة العالميَّة وفائدتها

كيف تعمل روبوتات الشَّبكة العالميَّة؟

تشتمل بنية الرُّوبوت عادةً على ما يلي

01

منطق التَّطبيق

هو الكود القابل للتَّنفيذ والقابل للقراءة آليًّا، الذي يكتبه مطوِّر الرُّوبوت ويُنفِّذه الحاسوب.

02

قاعدة البيانات

هي مجموعة البيانات التي يستمدّ منها الرُّوبوت معرفة الإجراءات التي يجب اتِّخاذها.

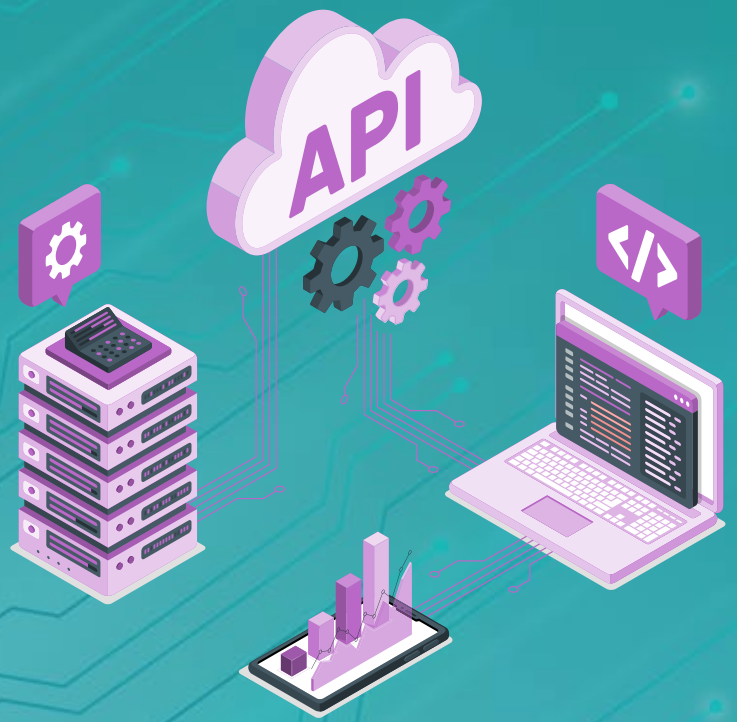
03

تكاملات API

تسمح واجهات برمجة التَّطبيقات للرُّوبوت باستخدام الوظائف الخارجيَّة دون أن يحتاج المطوِّر إلى كتابتها.

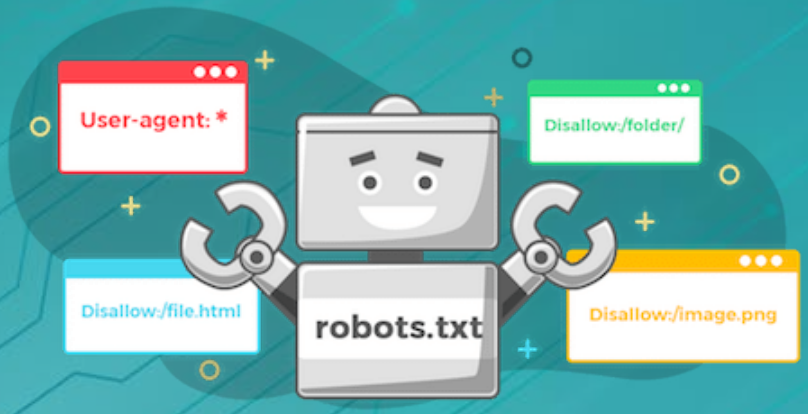
واجهة برمجة التَّطبيقات (API)

هي وسيلة لدمج الوظائف البرمجيَّة المُعقَّدة التي أنشأها شخص آخر بالفعل، على سبيل المثال، يمكن لروبوت الدَّردشة استخدام واجهة برمجة تطبيق الطَّقس لتوفير معلومات مُفصَّلة حول الطَّقس إذا طلب المُستخدِمون ذلك، وبهذه الطَّريقة لا يحتاج برنامج الدَّردشة الآليّ إلى تتبُّع الطَّقس نفسه، وبدلًا من ذلك يقوم فقط باستدعاء واجهة برمجة تطبيقات "تطبيق الطَّقس الخارجيّ".



ما ملفّ Robots.txt؟

هو ملفّ موجود على خادم ويب يُوضّح قواعد وصول الرُّوبوتات إلى الخصائص الموجودة على ذلك الخادم، فمن المُفترض أن يتّبع أيّ شخص يقوم ببرمجة الرُّوبوتات نظام الشَّرف ويتأكّد من أنّ الرُّوبوت الخاصّ به يتحقّق من ملفّ Robots.txt الخاصّ بموقع الويب قبل الوصول إلى موقع الويب، وبطبيعة الحال، لا تتّبع الرُّوبوتات الضَّارَّة هذا النِّظام عادةً، ومن هنا جاءت الحاجة إلى إدارة الرُّوبوتات.



إدارة الرُّوبوتات

تُشير إدارة الرُّوبوتات إلى حظر حركة مرور الرُّوبوتات غير المرغوب فيها أو الضَّارَّة على الإنترنت مع السَّماح للرُّوبوتات المفيدة بالوصول إلى خصائص الويب؛ حيث تُحقِّق إدارة الرُّوبوتات ذلك من خلال الكشف عن نشاط الرُّوبوتات، والتَّمييز بين سلوك الرُّوبوتات المرغوب فيه وغير المرغوب فيه، وتحديد مصادر النَّشاط غير المرغوب فيه.

أهمِّيَّة إدارة الرُّوبوتات

01

في حال ترك حركة الرُّوبوتات دون تحديد؛ يمكن أن تُسبِّب مشكلات هائلة لخصائص الويب.

02

تؤدِّي حركة مرور الرُّوبوتات الكبيرة جدًّا إلى وَضْع حِمْل ثقيل على خوادم الويب، ممَّا يتسبَّب في بُطء الخدمة أو رفضها للمُستخدِمين الشَّرعيِّين.

مديـر الرُّوبـوت

هو أيّ منتج برمجيّ يُدير الرُّوبوتات؛ حيث يكون مديرو الرُّوبوتات قادرين على حَظْر بعض الرُّوبوتات والسَّماح لآخرين بالمرور، بدلًا من مجرَّد حَظْر كلّ حركات المرور غير البشريَّة؛ لأنَّه في حال حَظْر جميع برامج الرُّوبوتات مثل برامج Google bot وعدم التَّمكُّن من فهرسة إحدى الصَّفحات؛ فلن تظهر هذه الصَّفحة في نتائج بحث Google، ما يعني انخفاض عدد الزِّيارات إلى موقع الويب.

أهداف مدير الرُّوبوت الجيِّد

- تمييز الرُّوبوتات من الزُّوَّار البشريِّين.
- تحديد سمعة البوت.
- تحديد عناوين IP الأصليَّة للبوت.
- تحليل سلوك الرُّوبوت.
- إضافة برامج الرُّوبوت النَّافعة إلى القوائم المسموح بها.
- الحدّ من استخدام الرُّوبوتات للخدمة بشَكْلٍ مُفرِط.
- رَفْض وصول الرُّوبوتات الضَّارَّة إلى محتويات معيَّنة.
- تقديم محتوًى بديل للرُّوبوتات.

ما فائدة روبوتات الشَّبكة العالميَّة؟

أتمتة المهامّ

تتفوَّق الرُّوبوتات في أتمتة المهامّ المُتكرِّرة، ممَّا يُوفِّر الوقت والجهد لكلٍّ من المؤسَّسات والأفراد.

كفاءة مُحسَّنة

تعمل الرُّوبوتات على مدار السَّاعة دون انقطاع، ممَّا يضمن توفُّر الخدمة بشَكْلٍ مستمرٍّ.

قابليَّة التَّوسُّع

يمكن للرُّوبوتات التَّعامُل مع عدد كبير من التَّفاعلات المتزامنة، ممَّا يجعلها حلولًا قابلة للتَّطوُّر بشَكْلٍ كبيرٍ.

تحليل البيانات

يمكن لروبوتات أتمتة المهامّ مُعالَجة كمِّيَّات هائلة من البيانات بسرعة ودقَّة، وهذا يُساعِد في جَمْع الرُّؤى واتِّخاذ القرارات المُستنِدة إلى البيانات.

تجربة مُستخدِم مُحسَّنة

في التِّجارة الإلكترونيَّة، يمكن لروبوتات الدَّردشة تقديم مساعدة شخصيَّة وتوجيه المُستخدِمين خلال العمليَّات واقتراح المنتجات أو الخدمات ذات الصِّلة بناءً على تفضيلاتهم.

حماية الأجهزة والملفَّات من الرُّوبوتات الضَّارَّة

علامات إصابة الأجهزة والملفَّات بشبكة الرُّوبوتات:

- انخفاض سرعة المُعالِج.
- تَعَطُّل التَّطبيق مكرَّرًا.
- بُطء سرعات الإنترنت.
- زيادة عدد منشورات وسائل التَّواصل الاجتماعيّ ورسائل البريد الإلكترونيّ غير المُصرَّح بها.
- ملاحظة وجود ملفَّات وتطبيقات غير مألوفة، التي لم تَقُمْ بتنزيلها أو تثبيتها.

ماذا تفعل إذا كان جهازك مصابًا ببرامج Botnet الضَّارَّة؟

- افْصِل جهازك عن أيّ شبكة Wi-Fi.
- تعرَّف على البرمجيات الضَّارَّة من خلال برنامج مكافحة الفيروسات، أو يمكنك البحث يدويًّا عن أيّ ملفَّات مشبوهة.
- قُمْ بإزالة البرمجيات الضَّارَّة تلقائيًّا أو يدويًّا، ويُفضَّل الأسلوب التِّلقائيّ؛ لأنَّه يضمن إزالة الملفَّات المُعدِية بالكامل من جهازك.
- أَعِد ضَبْط جهازك وأَعِد تثبيت نظام التَّشغيل الخاصّ بك.
- أَبلِغ عن إصابة الرُّوبوتات إلى السُّلطة المُختصَّة.

كيفيَّة مَنْع هجوم الرُّوبوتات

- تجنَّب النَّقر على الرَّوابط غير الموثوقة.
- تجنَّب تنزيل أيّ مرفقات بريديَّة من مُرسِلين لا تعرفهم.
- لا تَقُمْ بتنزيل البرامج من مصادر لم يتمّ التَّحقُّق منها، مثل البرامج المجانيَّة من الإنترنت.
- فَعِّل جدار الحماية على جهازك.
- قُمْ بتغيير إعدادات كلمات المرور الافتراضيَّة على أجهزتك الذَّكيَّة.
- احْتَفِظ بأجهزة إنترنت الأشياء الخاصَّة بك على شبكة Wi-Fi منفصلة.
- إعداد شبكة ضيف على جهاز توجيه Wi-Fi الخاصّ بك.
- قُمْ بتحديث نظام التَّشغيل والبرامج الأخرى بانتظام.
- قُمْ بتثبيت برنامج مكافحة الفيروسات.

أمثلة على هجمات الرُّوبوتات

EarthLink Spammer 2000

هو أوَّل مثال مُسَجَّل لهجوم الرُّوبوتات؛ حيث استُخْدِمَت فيه شبكة الرُّوبوتات غير المرغوب فيها لإرسال رسائل بريد إلكترونيّ إلى المُستخدِمين المطمئنِّين، على أمل الحصول على بيانات اعتمادهم الماليَّة.

Mariposa 2008

عبارة عن شبكة روبوتات إسبانيَّة تهدف إلى سرقة أرقام بطاقات الائتمان، وتضمَّنت ما يقرب من 10 ملايين جهاز في ذروتها، وهذا يجعلها واحدة من كبرى شبكات الرُّوبوتات التي تمّ اكتشافها على الإطلاق، وتمّ إسقاط شبكة الرُّوبوتات من قِبل سُلُطات إنفاذ القانون الإسبانيَّة التي تمكَّنت من اكتشاف الجُناة الذين يقفون وراءها.

Necurs Botnet 2012

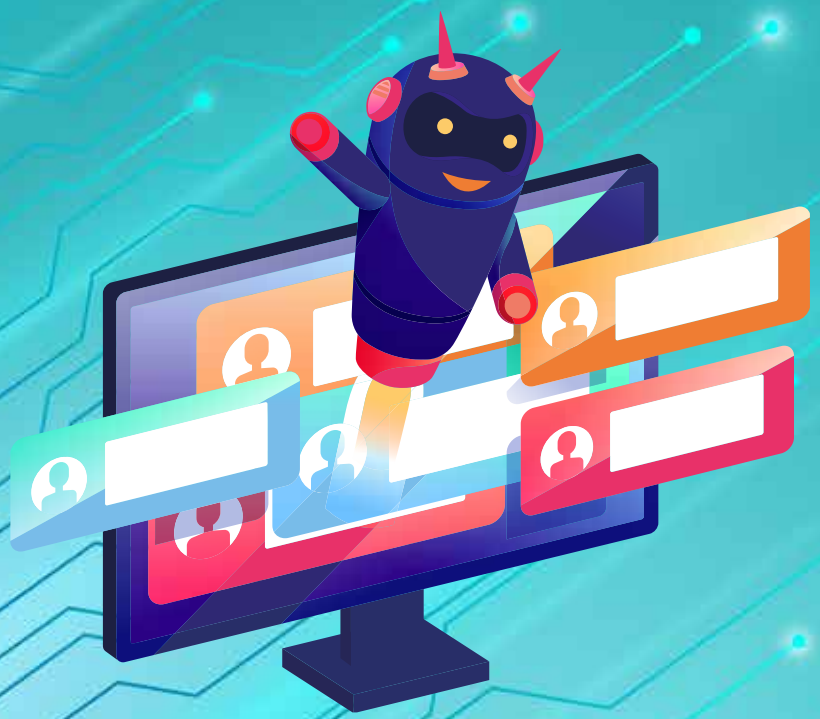
عبارة عن شبكة روبوتات ضخمة أصابت ما يقرب من تسعة ملايين جهاز حاسوب على مستوى العالم، وقد تمّ استخدامها لنَشْر البريد العشوائيّ والبرمجيات الضَّارَّة الخَطِرَة، بما في ذلك حصان طروادة المصرفيّ الشهير GameOver Zeus لكن تمّ تعطيل شبكة الرُّوبوتات Necurs بنجاح بواسطة Microsoft والوكالات الشَّريكة في عام 2020م.

Mirai Botnet 2016

تُعَدّ Mirai واحدة من أشهر هجمات الرُّوبوتات، واستهدفت على وجه التَّحديد الأجهزة الذَّكيَّة لأجهزة إنترنت الأشياء، وتمّ القبض على المبدِعين الأصليِّين لـ Mirai، إلَّا أنّ كود المصدر الخاصّ بها لا يزال موجودًا، وقد تمّ استخدامه لشنّ هجمات DDoS واسعة النِّطاق على مرّ السِّنين.

Glupteba Botnet 2019

هو نوع جديد من الرُّوبوتات يستهدف في المقام الأوَّل أجهزة Windows؛ لاستخراج العملات المُشفَّرة وسرقة بيانات اعتماد المُستخدِم، وقد قامت جوجل بتعطيل Glupteba في عام 2021م، لكنَّها عادت إلى الظُّهور منذ ذلك الحين، ممَّا يُشير إلى المرونة التي تُوفِّرها الهندسة القائمة على blockchain.



تمارين وتَدْريبَات

أولًا: التَّمَارين الصَّفِّيَّة

التَّمرين الأوَّل

أكمِل الجمل التَّالية

1. روبوتات الشَّبكة العالميَّة تُعْرف باسم ..... الويب أو ..... الإنترنت.

2. تقوم روبوتات الشَّبكة العالميَّة بعمل ..... تلقائيَّة على الإنترنت، وهي تُعَدّ من ..... التي تقوم بمهامّ ..... ومركَّبة، بصورة .....

3. تقوم روبوتات الإنترنت بعمل المهامّ البسيطة والمركَّبة بصورة متكرِّرة بمعدَّل ..... ممَّا يمكن أن يقوم به .....

4. المهمَّة الأساسيَّة لروبوتات الإنترنت هي ..... صفحات الإنترنت، حيث إنَّها مسؤولة عن جلب و ..... المعلومات من خوادم الويب بشَكْلٍ ..... وبسرعةٍ ..... أعلى من سرعة .....

5. كلّ خادم يحتوي على ملفّ ..... يقوم بعمليَّة الفهرسة، وهذا الملفّ يحتوي على كلّ القواعد التي تحكم سلوك ..... على ذلك الخادم.

6. تعتمد منصَّات التَّواصل الاجتماعيّ أيضًا على _____ الاجتماعيَّة، وهي عبارة عن _____ تتولَّى القيام بالعمليَّات _____ من أجل إنشاء خدمة أو _____ بين مستخدمي الشَّبكات الاجتماعيَّة.

7. البوتات الاجتماعيَّة تتبع _____ الدَّردشة و _____ التي تمّ تصميمها من أجل التَّحاور مع مستخدم _____

8. تمّ تصميم _____ الخاصَّة بمنصَّات التَّواصل _____ لكي تُقلِّد السُّلوكيَّات _____ من أجل جمع الأنماط _____ المشابهة لنمط المَستخدِم.

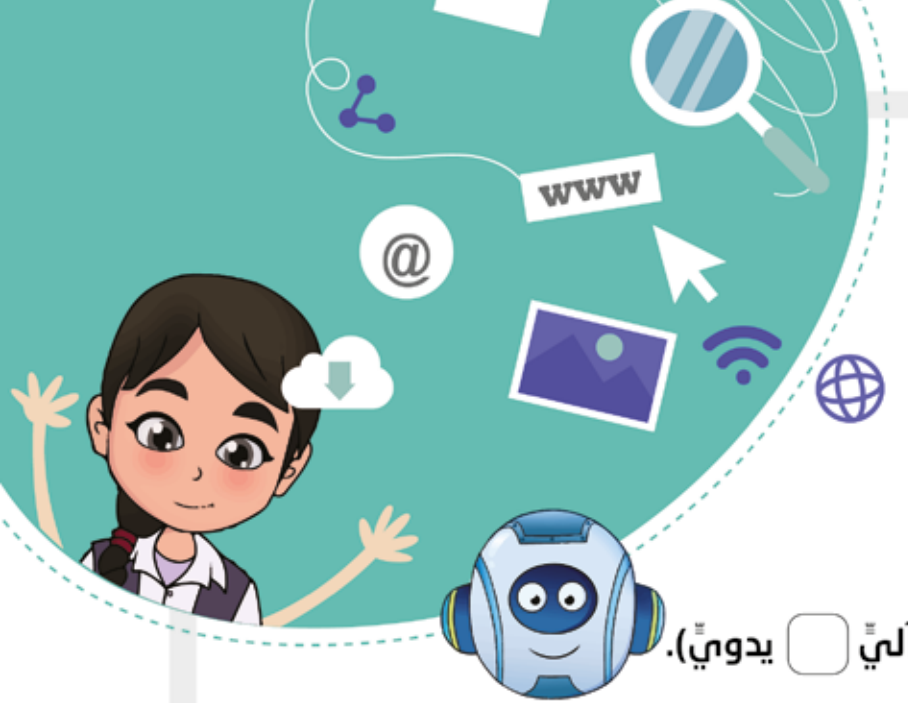
انْتَبِه!

الرُّوبوتات الضَّارَّة

هي عدد من الأجهزة المتَّصلة بالإنترنت، يعمل كلّ منها على تشغيل روبوت واحد أو أكثر، غالبًا دون عِلْم مالِكِي الأجهزة. ولأنّ كلّ جهاز له عنوان IP خاصّ به، فإنّ حركة مرور شبكة الرُّوبوتات تأتي من عناوين IP متعدِّدة؛ لذا يَصعُب تحديد مصدر حركة مرور الرُّوبوت الضَّار وحظره.

هل تعلم؟

الرُّوبوت المُستغلّ هو روبوت مُصمَّم لشراء منتجات أو خدمات سريعة الحركة بكمِّيَّات كبيرة؛ ما يجعل من الصَّعْب على العملاء الحقيقيِّين إكمال عمليَّات الشِّراء المشروعة.

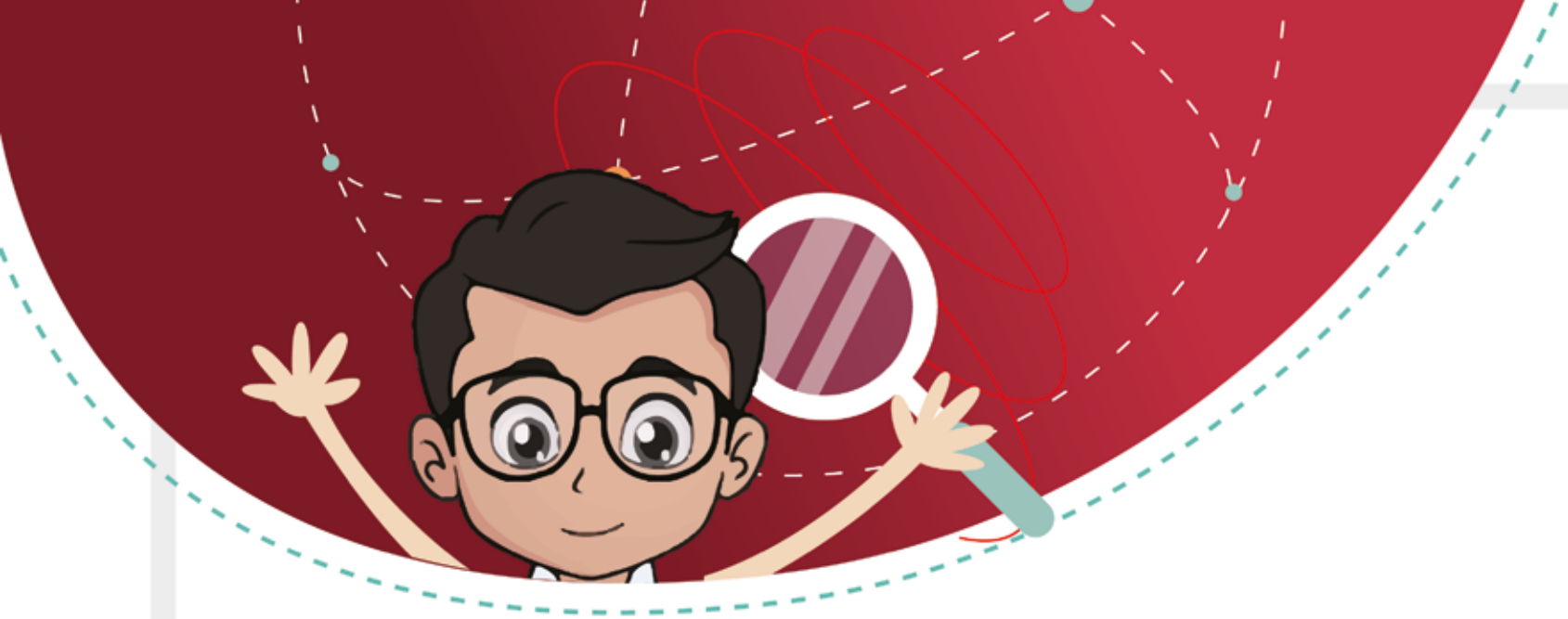


التَّمْرين الثَّاني

اخْتر الكلمة أو العبارة الصَّحيحة من الكلمات
أو العبارات الموجودة بين قوسين

- البوت هو اختصار لكلمة روبوت، وهو برنامج يقوم بالمهامّ بشَكْلٍ (☑ **آليٍّ** ☐ **يدويٍّ**).
- روبوتات الإنترنت تقوم بالمهامّ (☐ **بشَكْلٍ متكرّر** ☐ **مرّة واحدة فقط**) .
- سرعة روبوتات الإنترنت (☐ **تُماثِل السُّرعة البشريَّة** ☐ **أعلى من سرعة البشر**).
- تقوم روبوتات الإنترنت بالمهامّ (☐ **المفيدة** ☐ **غير المهمَّة**).
- من أهمّ المهامّ التي تقوم بها الرُّوبوتات هي (☐ **خدمة العملاء وفهرسة محرّكات البحث**

☐ **تأمين الحسابات الشَّخصيَّة للمُستخدِمين**).

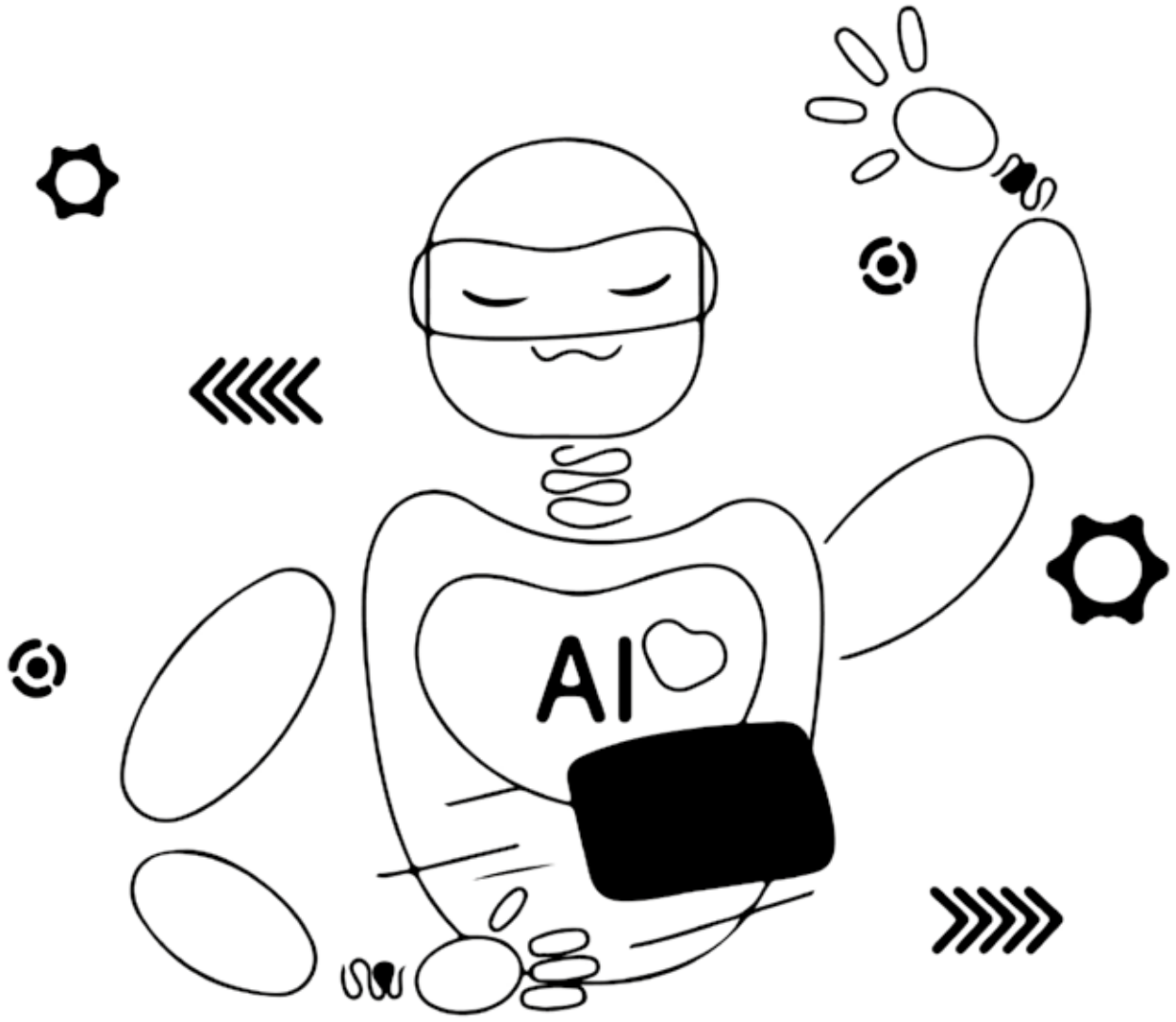


- بوتات الحاسوب تُعدّ (☐ **أداة رقميّة** ☐ **برنامج حماية**).
- أحيانًا تُستخدَم البوتات بشَكْلٍ خاطئٍ، ويتمّ استغلالها لمهاجمة (☐ **المواقع الإلكترونيّة** ☐ **الحسابات الشَّخصيّة**).
- يمكن لروبوتات الإنترنت أن (☐ **تُقلّد** ☐ **تتحكَّم في**) السُّلوك البشريّ.
- يمكن للبوتات الضَّارّة أن (☐ **تُشجّع** ☐ **تُقاطِع**) الأعمال وتُهاجم المواقع.
- يمكن لروبوتات الإنترنت أن تكون برمجيّات ضارّة إنْ (☐ **فقدت السَّيْطرة** ☐ **تحكَّمت بِشَكْلٍ كاملٍ**).

انْتَبِه!

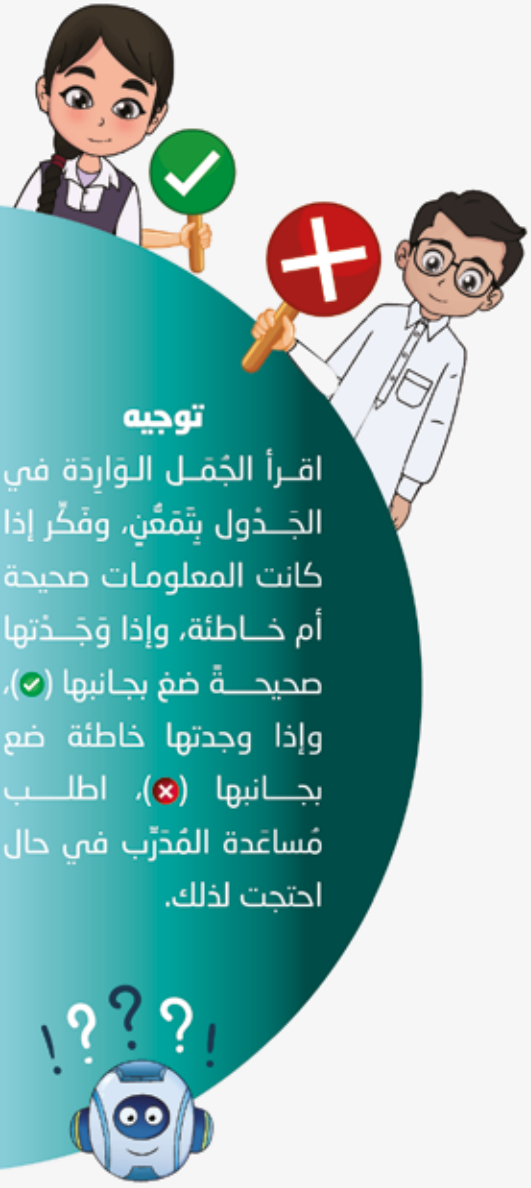
التَّنزيلات

إحدى الطُّرق الأكثر شيوعًا التي تُصيب بها الرُّوبوتات جهاز الحاسوب أو الهاتف الذَّكي أو الجهاز اللَّوحي الخاصّ بالمُستخدِم، حيث يتمّ تثبيت البَرْمَجيّات الضَّارَّة بتنسيق التَّنزيل عبر وسائل التَّواصل الاجتماعيّ أو رسائل البريد الإلكترونيّ التي تنصح بالنَّقر فوق الرَّابط، وغالبًا ما يكون الرَّابط على شكل صورة أو فيديو، ويحتوي إمَّا على فيروسات وإمَّا على بَرْمَجيّات ضارَّة أخرى.


AI

التَّمرين الثَّالث

ضع علامة (✓) بجانب العبارة الصَّحيحة، وعلامة (✗) بجانب العبارة الخاطئة.



توجيه

اقـرأ الجُمَـل الـوَارِدَة في الجَـدْول بِتَمَعُّنٍ، وفَكِّر إذا كانت المعلومات صحيحة أم خـاطئة، وإذا وَجَـدْتها صحيحـةً ضع بجانبها (✓)، وإذا وجدتها خاطئة ضع بجـانبها (✗)، اطلـب مُساعَدة المُدرِّب في حال احتجت لذلك.

1	روبوتات الشَّبكة العالميّة برامج لا تعمل إلّا بعد الحصول على إذن المُستخدِم.	
2	تقوم الرُّوبوتات بإنجاز المهامّ، كلّ مهمَّة على حِدَة.	
3	تُعْتبر روبوتات الإنترنت شديدة السُّرعة وأعلى كثيرًا من الأداء البشريّ.	
4	لا تقوم روبوتات الإنترنت إلّا بالمهامّ الضَّارَّة فقط.	
5	يمكن لروبوتات الإنترنت القيام بمهامّ خدمة العملاء وفهرسة المواقع.	

6 لا يمكن لروبوتات الإنترنت القيام بأيّ أعمال ضارّة.

7 أحيانًا تُهاجم روبوتات الإنترنت بعض المواقع الإلكترونيَّة الصَّغيرة فقط.

8 الشَّركات وحدها تستخدم روبوتات الإنترنت.

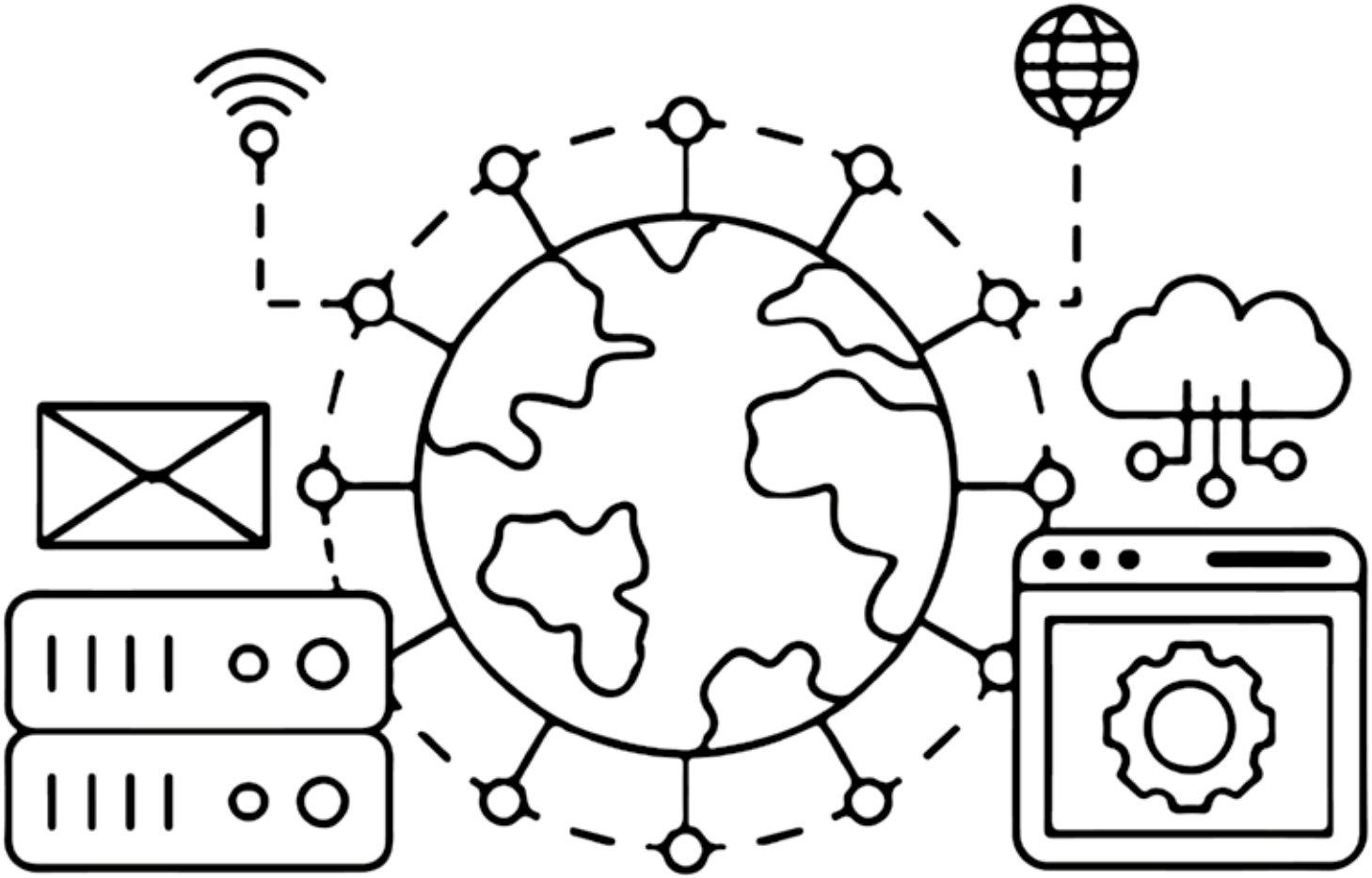
9 لا تقوم الرُّوبوتات إلَّا بـ 1% فقط من عمل شبكة الإنترنت في اليوم.

10 تُعْتبر الرُّوبوتات المسؤول الأوَّل عن تحسين محرِّكات البحث.

انْتَبِه!

Chatbots

هو روبوت صُمِّم للمشاركة في المحادثات مع المُستخدِمين، من خلال واجهات نصّيّة أو صوتيّة؛ حيث يستخدم تقنيّات مثل معالجة اللُّغة الطَّبيعيّة (NLP) والذَّكاء الاصطناعيّ (AI) لفَهْم استفسارات المُستخدِم وتقديم الاستجابات ذات الصِّلة.



التَّمرين الرَّابع

ضَعْ نوع البوت المناسب لكلّ جملة ممّا يلي

توجيه

اقْرأ العبارات الواردة في الجدول بدقّة، وفكِّر إلى أيّ نوع من أنواع البوتات تُشير العبارات، واكْتُب نوع البوت في العمود المقابل، أدناه مثال محلول.

1	هي بوتات تُحاكي المحادثات البشريّة عن طريق الرّد بجملٍ محدّدةٍ مسبقًا.	بوت الدَّرْدَشة
2	هي روبوتات تعمل على منصّات التّواصل الاجتماعيّ، وتُستخدَم في إنشاء الرّسائل التّلقائيّة والتّركيز على أفكار معيّنة ورصد الحسابات المزيّفة.	
3	هي بوتات تُساعِدك في العثور على أفضل الأسعار للمنتجات وتُراقب نمط الاستخدام لاقتراح منتجات معيّنة قد تناسبك.	
4	هي بوتات يمكنها فحص المحتوى الموجود على الإنترنت وتساعد في التّعامل مع المُستخدِمين والرّد على استعلاماتهم.	
5	هي بوتات تقرأ البيانات من المواقع الإلكترونيّة ويمكنها حفظها من أجل استخدامها أو إعادة استخدامها، وغالبًا ما تساعد في منع سرقة المعلومات وحماية حقوق الطّبْع والنّشْر.	

6	هي روبوتات متخصّصة في جمع المعلومات الخاصَّة بالمستخدمين من خلال زيارة المواقع الإلكترونيَّة بشَكْلٍ آليٍّ لاستعادة المعلومات والإجابة عن أسئلة معيَّنة.	
7	هي روبوتات تُستخدَم في مراقبة صحَّة المواقع أو الأنظمة، وتساعد في توفير المعلومات في الوقت الفعليّ.	
8	هي روبوتات تُستخدَم في إكمال المعاملات بالنِّيابة عن المَستخدِمين من البشر، ومن خلالها يمكن للمُستخدِم أن يُجرِي المعاملة في سياق المحادثة.	
9	هي بوتات تُستخدَم في تنزيل البرامج أو التَّطبيقات بشَكْلٍ آليٍّ من المتاجر المتخصّصة في التَّطبيقات.	
10	هي بوتات تعمل بشَكْلٍ تلقائيّ على شراء التَّذاكر في الفعاليَّات المشهورة من أجل إعادة بيع تلك التَّذاكر للتَّربح منها، ويُعَدّ هذا نشاطًا غير شرعيّ في كثير من الدُّول في أنحاء العالم.	

انْتَبِه!

روبوتات أتمتة المهامّ

نوع من الرُّوبوتات يُركّز على أتمتة المهامّ شائعة الاستخدام ومعالجة البيانات، وغيرها من الأنشطة الروتينيّة التي قد تستغرق وقتًا طويلًا من البشر.

هل تعلم؟

"روبوتات حَشْو بيانات الاعتماد" تستطيع الوصول إلى حسابات المُستخدِمين عن طريق شنّ هجمات من خلال استخدام أسماء المُستخدِمين وكلمات المرور المسروقة أو خَرْق حسابات المُستخدِمين.

التَّمرين الخامس

صنِّف الرُّوبوتات التَّالية إذا كانت (ضارَّة) أم (نافعة)

• البريد المزعج Spam.	ضارَّة
• بوتات العناكب أو زواحف الشَّبكة.	
• الدَّردشة لخداع الأشخاص.	
• بوتات مشاركة الملفَّات.	
• بوتات التَّذاكر.	
• بوتات المراقبة.	
• بوتات المعاملات.	
• إدخال بيانات الاعتماد.	
• هجمات الحرمان من الخدمة.	
• بوتات التَّنزيل.	
• بوتات زواحف سرقة المحتوى.	

- بوت المحادثة للرَّدّ الآليّ.
- هجمات الحرمان من المخزون.
- جامعو المعلومات.
- فاحصات نقاط الضَّعف.
- بوتات المتاجر.
- بوتات النَّقرات الاحتياليَّة.
- مراقبة النَّشاط.
- البوتات الاجتماعيَّة.

انْتَبِه!

روبوتات محرِّك البحث

من أنواع الرُّوبوتات النَّافعة، وتُعرف أيضًا باسم "برامج زحف الويب"، ويتمّ استخدامها بواسطة محرِّكات البحث الشَّهيرة، مثل Google وYahoo وBing، للزَّحف إلى الإنترنت والعثور على المعلومات التي يحتاج إليها المُستخدِم.

التَّمرين السَّادس

الجمل التَّالية خاطئة؛ حدِّد الأخطاء ثمّ قُمْ بتصحيحها.

لا يمكن للبوتات الموجودة على الإنترنت التَّواصل مع بعضها.

يمكن للبوتات الموجودة على الإنترنت التَّواصل مع بعضها.

تُعْتبر الخوارزميّات جزءًا غير أساسيّ في البوتات ولا أهمّيّة كبيرة لها.

تعمل بوتات المحادثة بشَكْلٍ تلقائيّ دون أوامر محدَّدة مسبقًا.

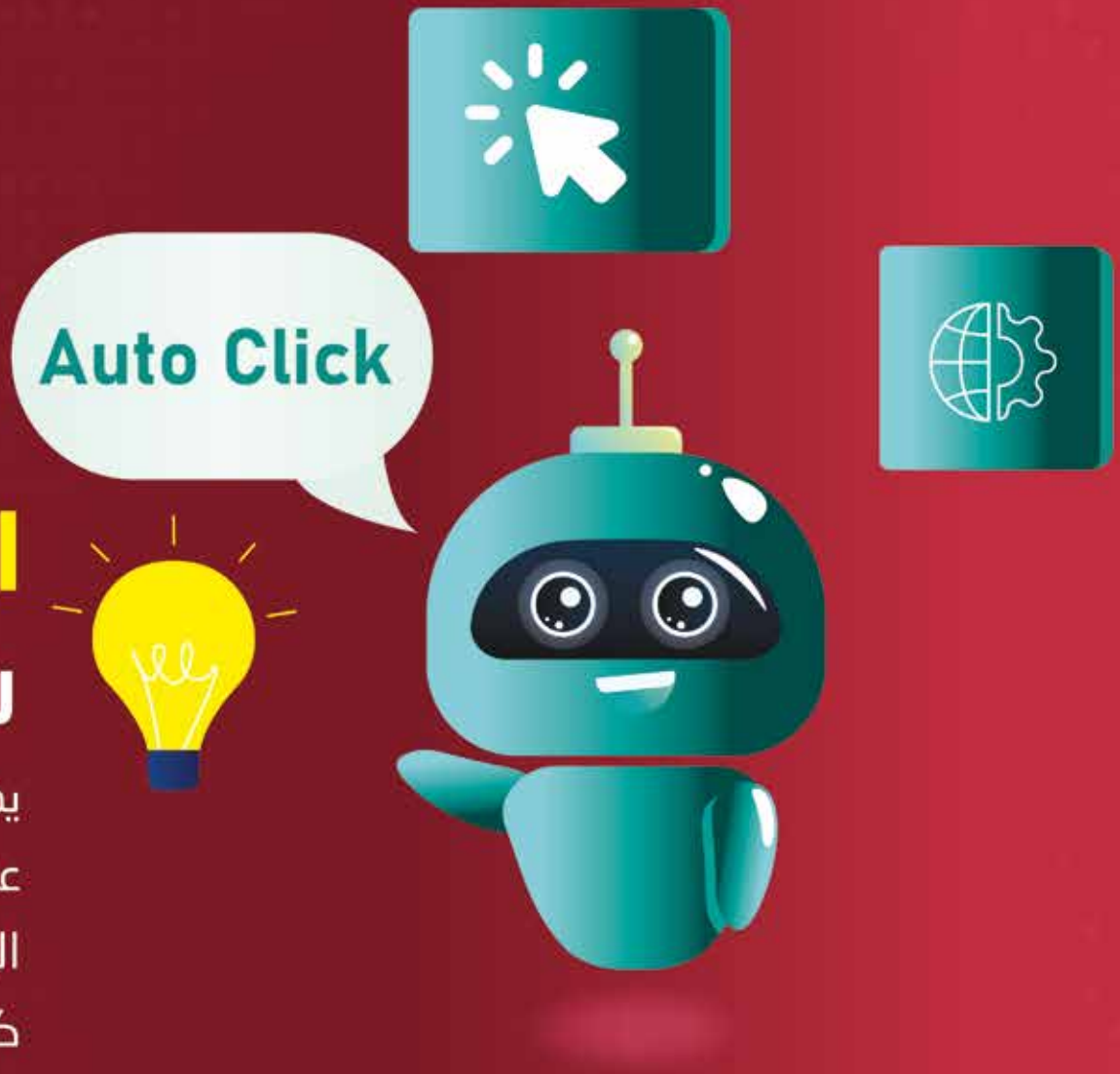
توجيه

اقْرأ الجمل الواردة بتمعُّن، وحدِّد الخطأ الموجود في كلّ جملة وقُمْ بتصحيحه، ثمّ وَضْع مثال محلول.

لا يمكن للبوتات التَّعلُّم من البشر.

لا تستخدم البوتات تقنيّات الذَّكاء الاصطناعيّ.


ثانيًا: التَّمارين اللَّاصَفِّيَّة



انْتَبِه!

روبوتات النَّقر

يمكن لـروبوتات Clickbots النَّقر تلقائيًّا على الرَّوابط الموجودة على مواقع الويب، ممَّا يؤدِّي إلى إنشاء حركة مرور كبيرة، ما يتسبَّب في خداع المعلنين من خلال نقرات المُستخدِم المصطنعة، فهي تخدع تصنيفات محرِّك البحث.

التَّمرين الأوَّل

صنِّف الجمل التَّالية حسب ما إذا كانت عيوبًا أم مزايا للبوتات.

توجيه

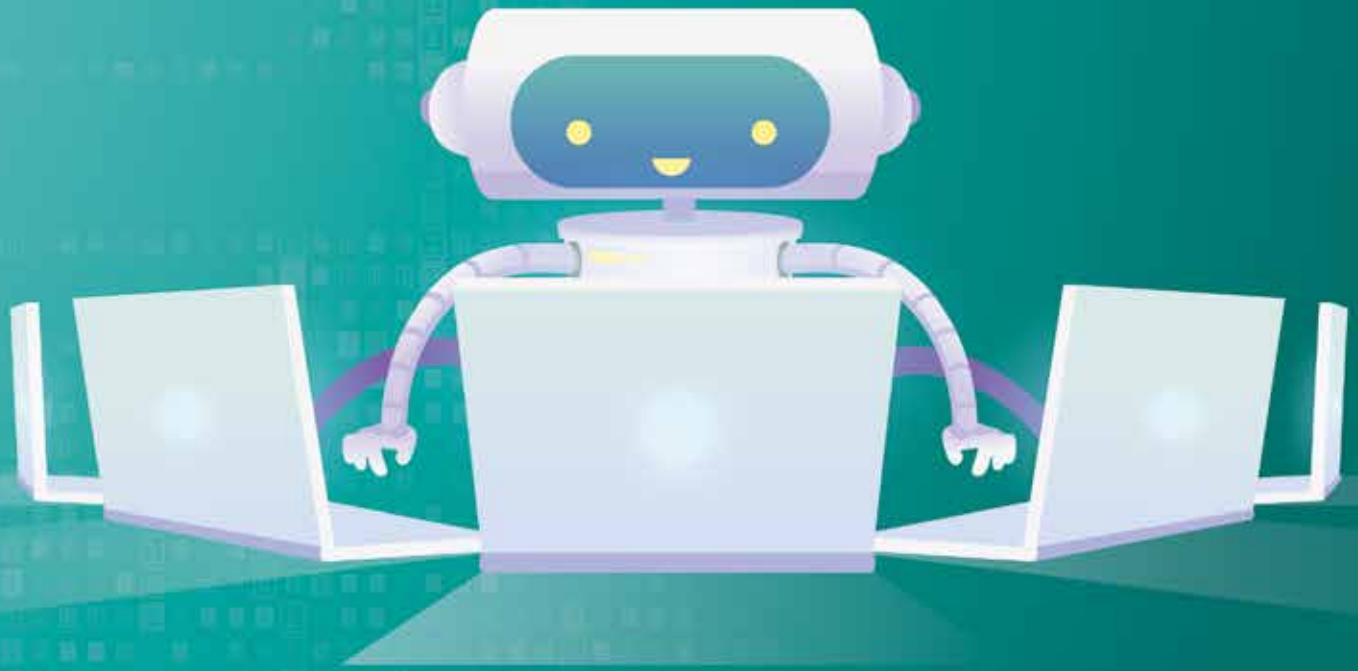
اقْرأ الجمل الواردة بتمعُّن، وحدِّد ما إذا كانت تُعبِّر عن عيوب أم مزايا للبوتات، ويوجد مثال محلول.

1. أسرع من البشر، خاصَّةً في المهامّ المتكرِّرة والنَّمطيَّة.	**ميزة**
2. تُوفِّر وقتًا للعملاء والزَّبائن.	
3. تُقلِّل من تكاليف العِمالة للشَّركات.	
4. قد تكون برمجتها خبيثة.	
5. لا يمكنها تأدية كلّ المهامّ، وقد يتسبَّب الجهل بها في المخاطر.	
6. متاحة على مدار السَّاعة.	
7. يمكن أن تُستخدَم في البريد العشوائيّ.	
8. تُمكِّن الشَّركات من الوصول إلى أعداد أكبر من الجمهور، عن طريق تطبيقات المراسلة.	
9. قابلة للتَّخصيص.	
10. لا يمكنها العمل دون إدارة بشريَّة تتدخَّل في بعض الأحيان.	
11. متعدِّدة الأغراض.	
12. يمكنها أن تُحسِّن من تجربة المُستخدِم.	

انْتَبِه!

مجمِّعو البيانات

هي روبوتات مصمَّمة لجَمْع المعلومات من مصادر مختلفة وإنشاء أدلَّة شاملة أو قوائم محتوى؛ حيث تقوم هذه الرُّوبوتات بجَمْع البيانات وتحديثها لتزويد المُستخدِمين بمعلومات مُحدَّثة بشأن مواقع الويب أو الشَّركات أو المنتجات أو الخدمات.



التَّمرين الثَّاني

رتِّب الخطوات التَّالية في حال تعرّض جهاز الحاسوب الخاصّ بك لفيروس بوت.

توجيه

اقرأ الجمل الواردة أدناه بتمعُّن، وحدِّد الجملة التي تُشير إلى التَّصرُّف الأوَّل في حال التَّعرُّض لفيروس بوت، والثَّانية والثَّالثة وهكذا حتى نهاية الجمل.

1	انقل جميع البيانات المهمّة أو الشَّخصيّة إلى جهاز آخر أو قرص صلب خارجيّ.	
2	نَظِّف الحاسوب باستخدام أدوات الأمان المختلفة، أو اطْلُب من محترفٍ فِعل هذا.	
3	افْصِل الحاسوب من الشَّبكة في أسرع وقتٍ ممكن؛ لوقف سرقة البيانات والمعلومات.	
4	أَعِد ضبط المصنع لجهازك، وبهذا ستتخلّص من المشكلة، وللأسف ستُحْذَف كافّة الملفّات على جهازك.	

التَّمرين الثَّالث

ضع علامة (✓) بجانب العبارة الصَّحيحة،
أو علامة (✗) بجانب العبارة الخاطئة وصحّح العبارة الخاطئة.

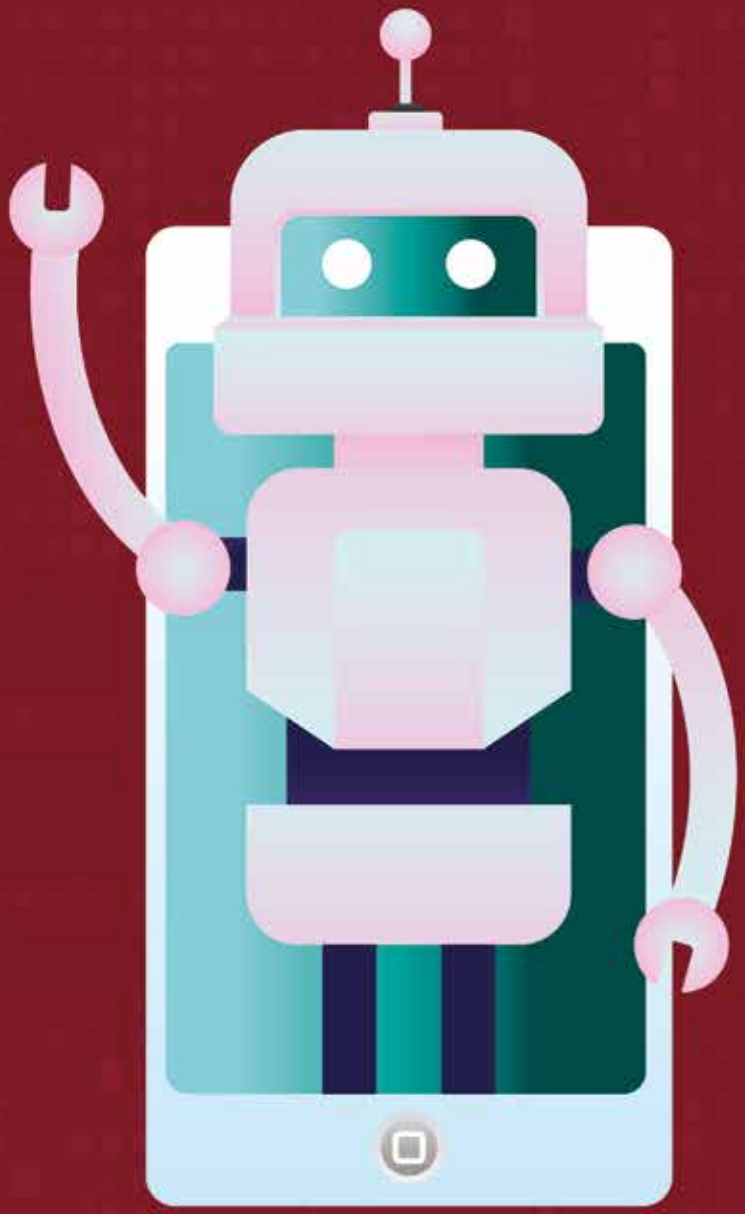
1. لا يمكنك بأيّ حال من الأحوال أن تحمي جهازك من هجمات البوتات.
   يمكنك حماية جهازك من هجمات البوتات. ✗
2. تثبيت برامج مكافحة البرمجيّات الضَّارّة يساعد على حماية جهازك من هجمات البوتات. ✓
3. إهمال التَّحديثات الخاصَّة بالبرامج لا يؤثّر في أيّ شيء. ✗
4. استخدام كلمات مرور قويَّة يساعد على تجنُّب كثير من المشكلات الأمنيَّة. ✓

5 يمكنك النَّقر على الرَّوابط الموجودة على الشَّبكة العنكبوتيَّة دون خوف.

6 لا توجد مواقع إلكترونيَّة أو إعلانات غير موثوقة.

7 من المهمّ تثبيت جدار ناريّ للمساعدة على حَجْب الهجمات الخبيثة.

8 استخدام برنامج مدير البوتات لا يؤثّر في البوتات الضَّارّة.



انْتَبِه!

هجوم الرُّوبوت

نوع من الهجمات الإلكترونيَّة التي تستخدم البرمجيَّات النَّصِّيَّة الآليَّة لتعطيل الموقع أو سرقة البيانات أو إجراء عمليَّات شراء احتياليَّة أو تنفيذ إجراءات ضارَّة أخرى، ويمكن نَشْر هذه الهجمات ضدّ عدد من الأهداف المختلفة، مثل مواقع الويب والخوادم والتَّطبيقات، ويختلف غرض هذه الهجمات، لكنَّها غالبًا ما تتضمَّن سرقة معلومات حسَّاسة أو التَّسبُّب في تلف البنية التَّحتيَّة للهدف أو الإضرار بالسُّمعة.

هل تعلم؟

"برامج زحف الويب" هي برامج تستخدم الرُّوبوتات للزَّحف إلى الإنترنت والعثور على المعلومات التي يحتاج إليها المُستخدِم.

انْتَبِه!

سرقة الويب/المحتوى Web/content scraping

يُقصَد بها قيام الرُّوبوت بتنزيل معظم المحتوى الموجود على موقع الويب أو كلِّه، بغضّ النَّظر عن رغبات مالِك موقع الويب، بواسطة الرُّوبوتات الآليَّة، وغالبًا ما تُستخدَم روبوتات استخراج المحتوى لإعادة توظيف المحتوى لأغراض ضارَّة، مثل تكرار المحتوى لتحسين محرِّكات البحث على مواقع الويب التي يمتلكها المُهاجِم، وانتهاك حقوق الطِّباعة، والنَّشْر والتَّجسُّس على حركة مرور البيانات.

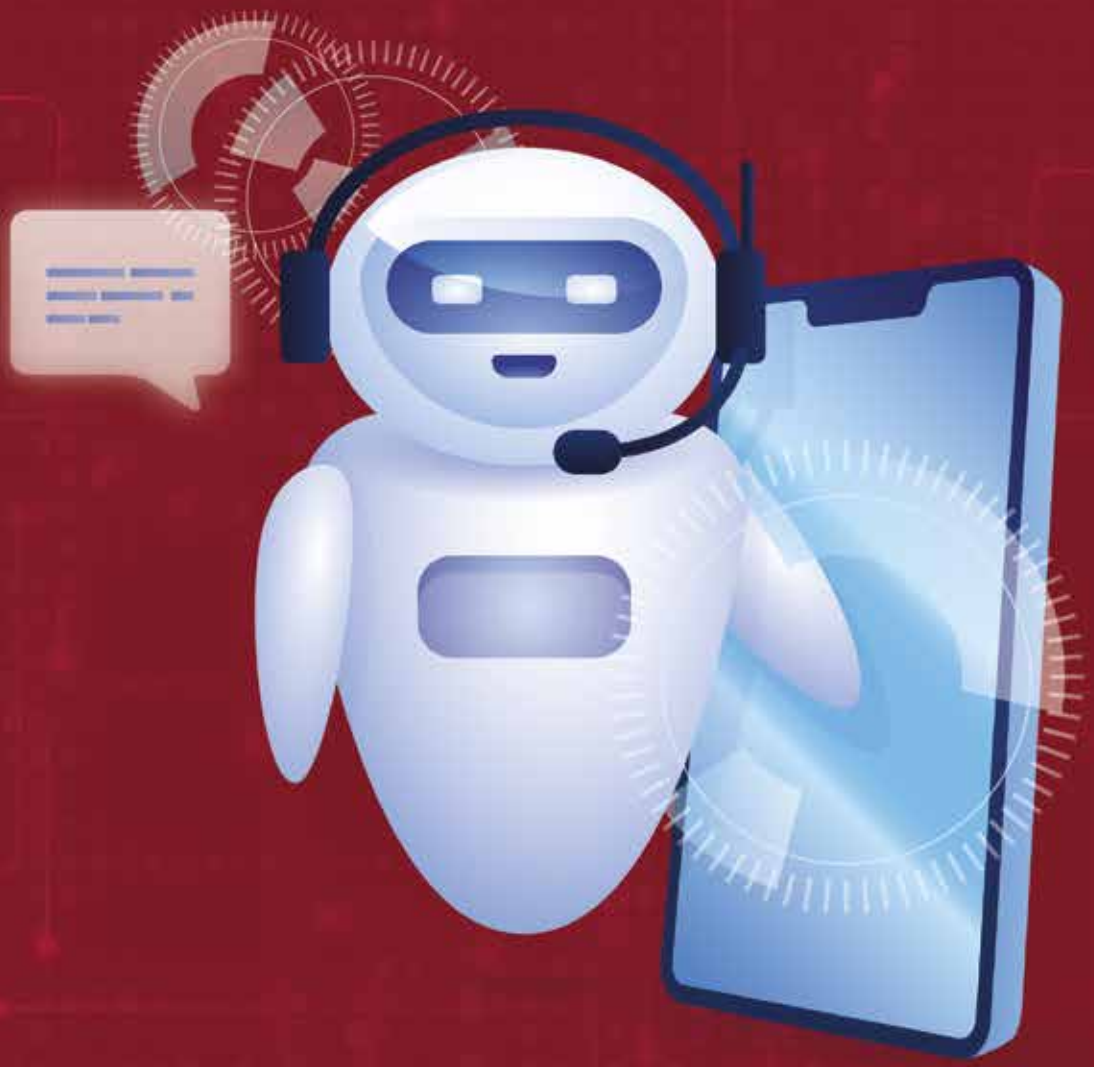
التّمرين الرّابع
استخرج الكلمات التّالية من الجدول:

توجيه
اقرأ الكلمات الواردة أدناه بتمعُّن، وابحث في الجدول عن حروف متتالية تُشكِّل هذه الكلمات، وأدناه مثال عن كلمة **"روبوتات"** وكيف تمّ إيجاد أحرف الكلمة في الجدول:

م	ح	ر	ك	ا	ت	ا	ل	ب	ح	ث
ا	ل	ض	ا	ر	ة	ل	غ	ف	ق	م
ل	ا	ل	ع	ا	ل	م	ي	ة	ك	و
ت	ل	ق	ا	و	ي	س	م	ه	و	ق
ر	و	ب	و	ت	ا	ت	س	ر	ي	ع
ا	ل	م	ف	ي	د	خ	ا	غ	ي	ب
م	ت	ك	ر	ر	ة	د	ت	خ	د	ح
س	ا	ل	ا	ج	ت	م	ا	ع	ي	ة
ا	ل	ا	ف	ر	ا	د	ف	ت	ر	ي
ر	س	ا	ئ	ل	ر	ق	م	ي	ة	ش
ا	ل	ش	ر	ك	ا	ت	و	و	ن	ت

روبوتات - سريع - المُستخدِم -الاجتماعيَّة - العالميَّة - الضَّارَّة - المفيد - متكرِّرة - رقميَّة - رسائل

موقع - محرّكات البحث - الشَّركات - الأفراد



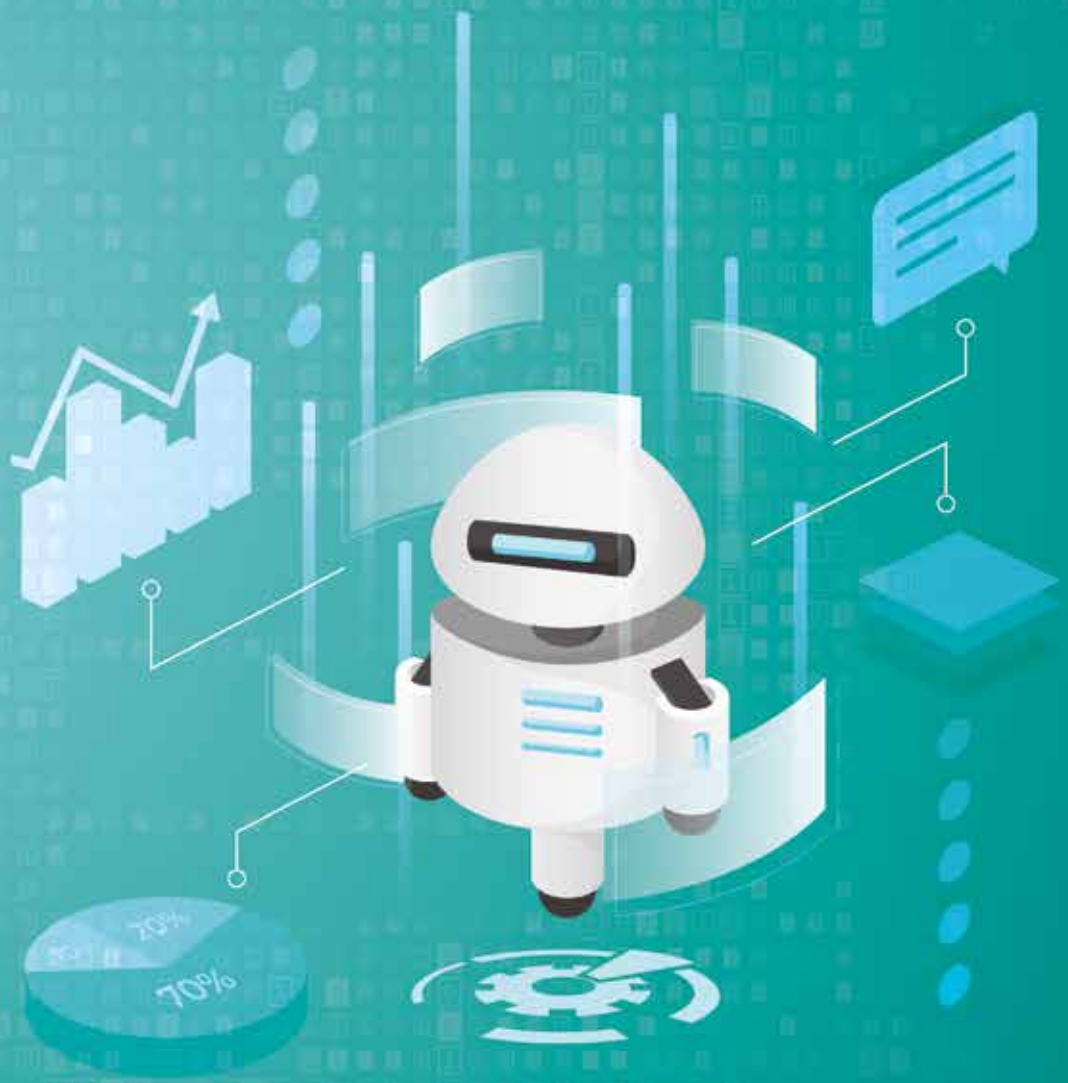
انْتَبِه!

روبوتات سرقة بيانات الاتصال

من أنواع الرُّوبوتات الضَّارَّة، وتقوم بفحص مواقع الويب بحثًا عن معلومات الاتِّصال، مثل أرقام الهواتف وعناوين البريد الإلكترونيّ، ثمّ تنزيل تلك المعلومات. وتُعَدّ روبوتات تجميع البريد الإلكترونيّ نوعًا من برمجيّات السَّرقة التي تَستهدِف عناوين البريد الإلكترونيّ على وَجْه التَّحديد، وذلك عادةً بغرض العثور على أهداف جديدة للبريد العشوائيّ.

هل تعلم؟

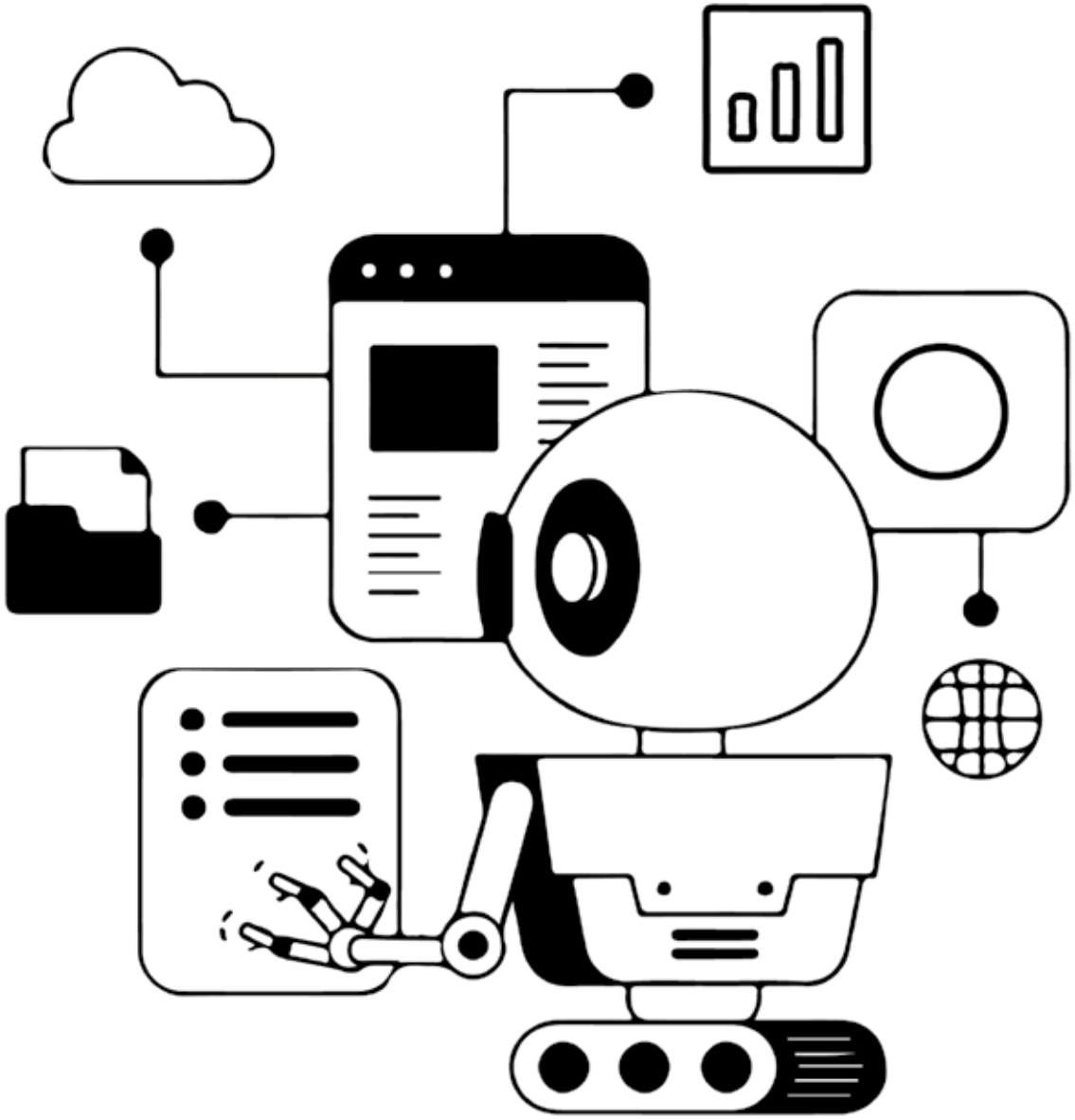
بُطء شبكة الإنترنت يُعَدّ من علامات إصابة الأجهزة والملفَّات بهجمات الرُّوبوتات.

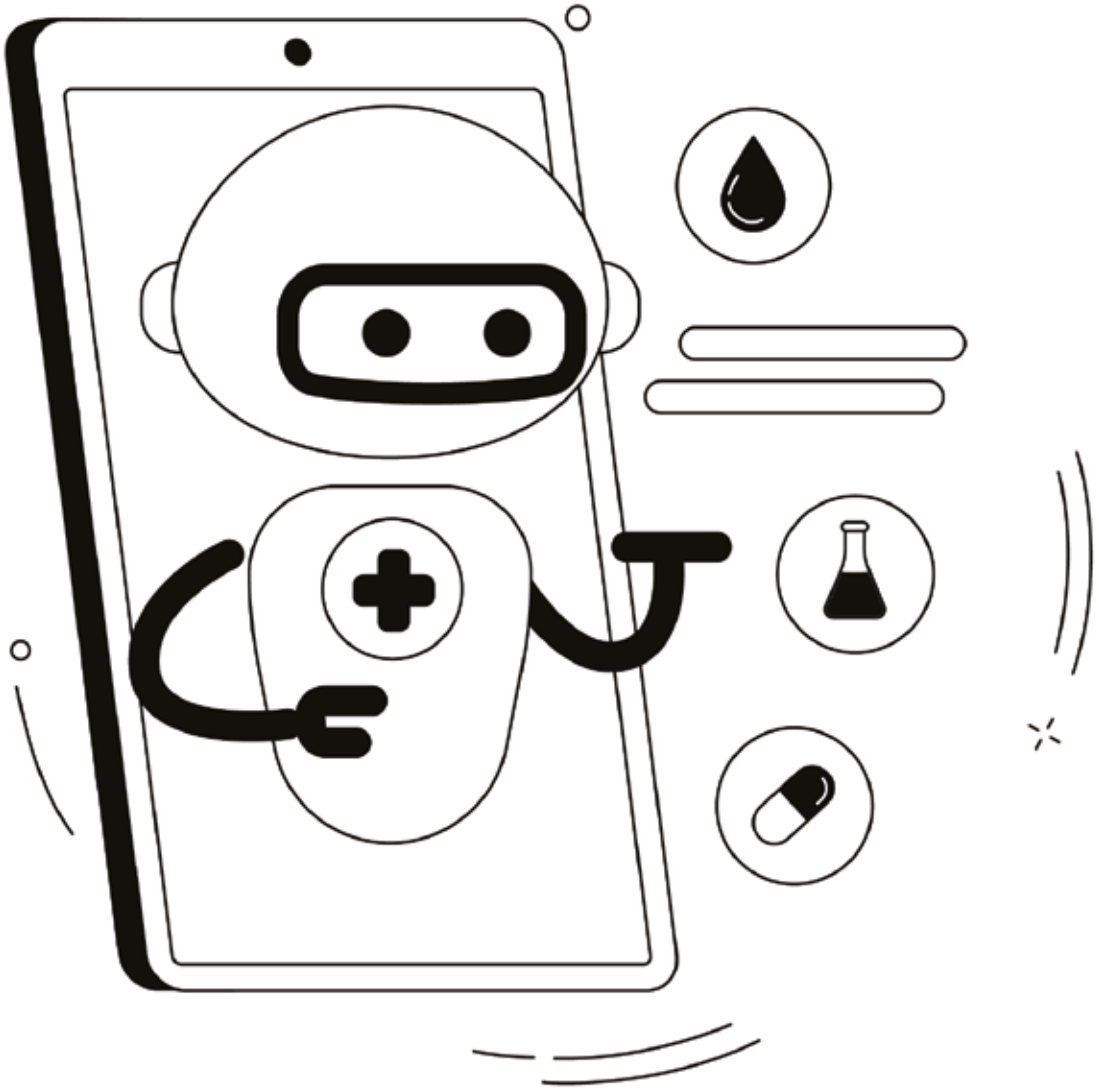


انْتَبِه!

إدارة الرُّوبوتات

تُشير إدارة الرُّوبوتات إلى حظر حركة مرور الرُّوبوتات غير المرغوب فيها أو الضَّارَّة على الإنترنت مع السَّماح للرُّوبوتات المفيدة بالوصول إلى خصائص الويب؛ حيث تُحقِّق إدارة الرُّوبوتات ذلك من خلال الكشف عن نشاط الرُّوبوتات، والتَّمييز بين سلوك الرُّوبوتات المرغوب فيه وغير المرغوب فيه، وتحديد مصادر النَّشاط غير المرغوب فيه.





انْتَبِه!

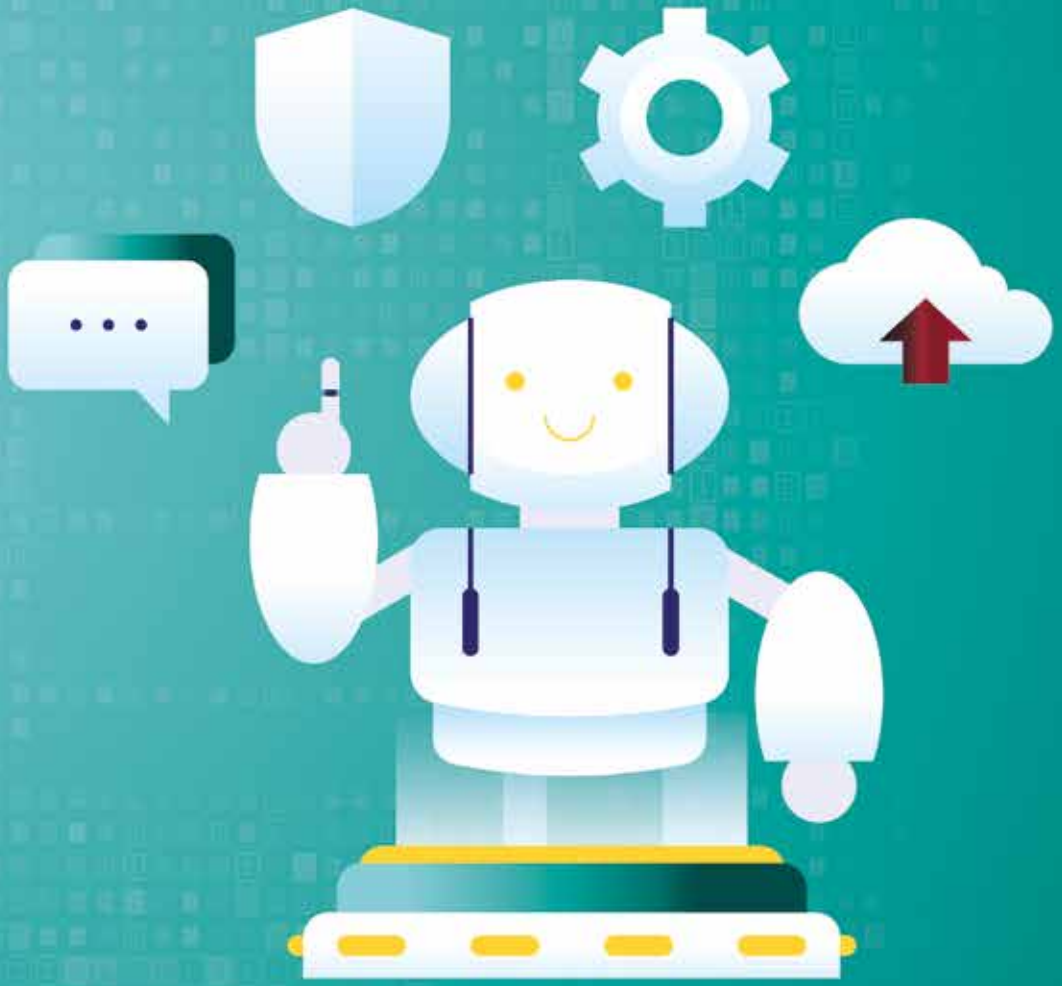
ملفّ Robots.txt

هو ملفّ موجود على خادم ويب يُوضّح قواعد وصول الرُّوبوتات إلى الخصائص الموجودة على ذلك الخادم، فمن المفترض أن يتّبع أيّ شخص يقوم ببرمجة الرُّوبوت نظام الشَّرف ويتأكّد من أنّ الرُّوبوت الخاصّ به يتحقّق من ملفّ Robots.txt الخاصّ بموقع الويب قبل الوصول إلى موقع الويب، وبطبيعة الحال، لا تتّبع الرُّوبوتات الضَّارّة هذا النِّظام عادةً، ومن هنا جاءت الحاجة إلى إدارة الرُّوبوتات.

انْتَبِه!

مدير الرُّوبوت

هو أيّ منتج برمجيّ يُدير الرُّوبوتات؛ حيث يكون مديرو الرُّوبوتات قادرين على حظر بعض الرُّوبوتات والسَّماح لآخرين بالمرور، بدلًا من مجرَّد حظر كلّ حركة المرور غير البشريَّة؛ لأنَّه عند حظر جميع برامج الرُّوبوت مثل برامج Google bot ولم يتمكَّن من فهرسة إحدى الصَّفحات، فلن تظهر هذه الصَّفحة في نتائج بحث Google، ما يعني انخفاض عدد الزِّيارات إلى موقع الويب.



انْتَبِه!

روبوتات الاستيلاء على الحساب (ATO)

تُعْرف أيضًا باسم "روبوتات حَشْو بيانات الاعتماد"، وتستطيع الوصول إلى حسابات المُستخدِمين عن طريق شنّ هجمات حَشْو بيانات الاعتماد، من خلال استخدام أسماء المُستخدِمين وكلمات المرور المسروقة أو خَرْق حسابات المُستخدِمين باستخدام المعلومات الحسّاسة مثل تفاصيل بطاقة الائتمان والحساب المصرفيّ.

مخاطر الرُّوبوتات الضَّارَّة

تراجُع الثِّقة.

الاحتيال والسَّرقة.

التَّلاعب بالمحتوى.

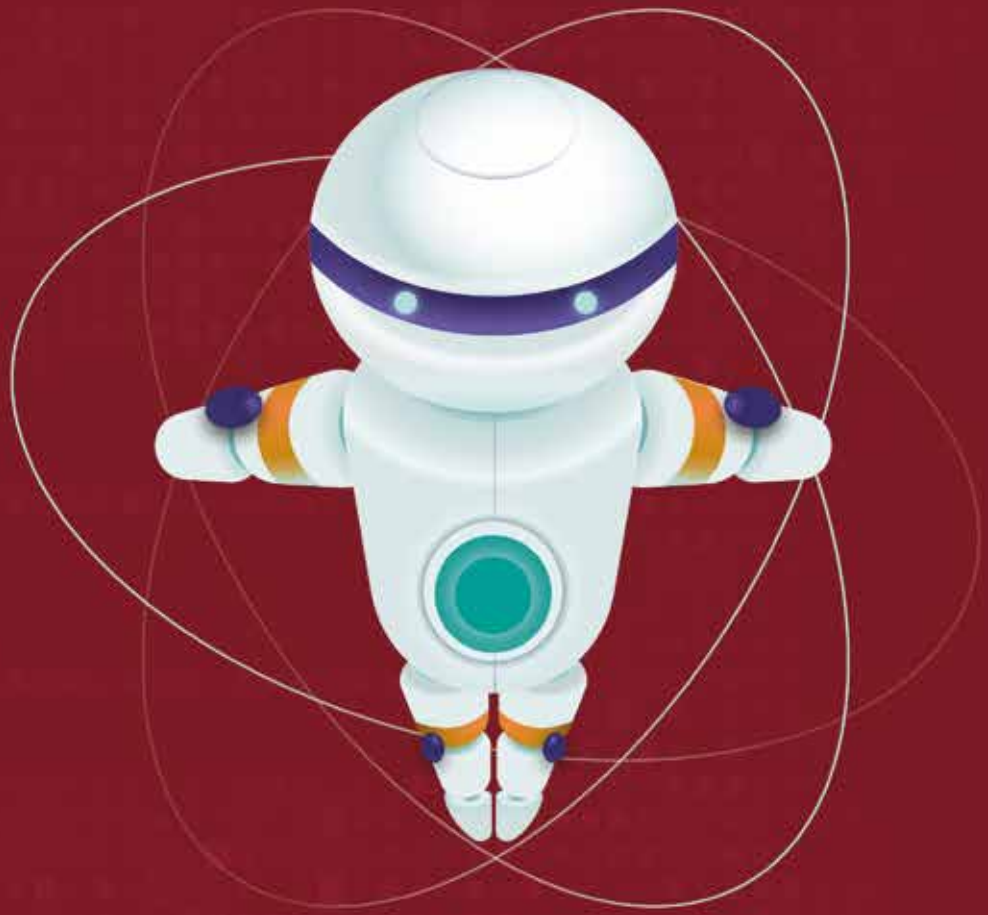
انتهاكات خصوصيَّة البيانات.

هجمات منع الخدمة المُوزَّعة (DDoS).

مميِّزات الرُّوبوتات في النِّظام البيئيّ الرَّقميّ

1. الكفاءة.
2. إضفاء الطَّابع الشَّخصيّ.
3. التَّوفُّر.
4. انخفاض التَّكلِفة.
5. قابليَّة التَّوسُّع.

منافع روبوتات وسائل التَّواصل الاجتماعيّ



1. إنشاء منشورات وسائل التَّواصل الاجتماعيّ ونَشْرها.
2. جمع معلومات المَستخدِم.
3. توفير دعم العملاء.

علامات إصابة الأجهزة والملفّات بهجوم الرُّوبوتات

- بُطء سرعة الإنترنت.
- انخفاض في سرعة المُعالِج.
- أعطال التَّطبيقات المُتكرِّرة.
- وجود ملفّات وتطبيقات غير مألوفة.
- زيادة عدد منشورات وسائل التَّواصل الاجتماعيّ ورسائل البريد الإلكترونيّ غير المُصرَّح بها.

ماذا تفعل إذا كان جهازك مصابًا ببرمجيَّات Botnet الضَّارَّة؟

- افْصِل جهازك عن شبكة الإنترنت.
- قُمْ بإزالة البرمجيَّات الضَّارَّة تلقائيًّا أو يدويًّا.
- الإبلاغ عن إصابة الرُّوبوتات إلى السُّلطة المُختصَّة.
- أَعِد ضبط جهازك وأَعِد تثبيت نظام التَّشغيل الخاصّ بك.
- التَّعرف على البرمجيَّات الضَّارَّة من خلال برنامج مكافحة الفيروسات وإزالتها.

كيفيّة منع هجوم الرُّوبوتات

- تشغيل جدار الحماية على جهازك.
- تجنّب النّقر على الرّوابط المشبوهة.
- قُمْ بتثبيت برنامج مكافحة الفيروسات.
- لا تقم بتنزيل البرامج من مصادر لم يتمّ التّحقّق منها.
- قُمْ بتحديث نظام التّشغيل والبرامج الأخرى بانتظام.
- إعداد شبكة ضيف على جهاز توجيه Wi-Fi الخاصّ بك.
- تجنّب تنزيل أيّ مرفقات بريديّة من مُرسِلين لا تعرفهم.
- احتفظ بأجهزة إنترنت الأشياء الخاصّة بك على شبكة Wi-Fi منفصلة.


أسئلة
المسابقات

مـا هــو؟

هو برنامج يَنفّذ مهامّ تلقائيّة ومتكرّرة ومحدَّدة مسبقًا، وعادةً ما يُقلِّد سلوك المَستخدِم البشريّ أو يحلّ محلّه لكنّه يعمل بشَكْلٍ أسرع بكثير من البشر.

عبارة عن عدد من الأجهزة المتّصلة بالإنترنت، ويعمل كلّ منها على تشغيل روبوت واحد أو أكثر، وذلك غالبًا دون علم مالِكي الأجهزة؛ لأنّ كلّ جهاز له عنوان IP خاصّ به؛ لذا يَصْعُب تحديد مصدر حركة مروره.

روبوت مُصمَّم للمشاركة في المحادثات مع المُستخدِمين، وذلك عادةً من خلال واجهات نصّيّة أو صوتيّة؛ حيث يستخدم تقنيّات مثل معالجة اللُّغة الطَّبيعيّة (NLP) والذَّكاء الاصطناعيّ (AI).

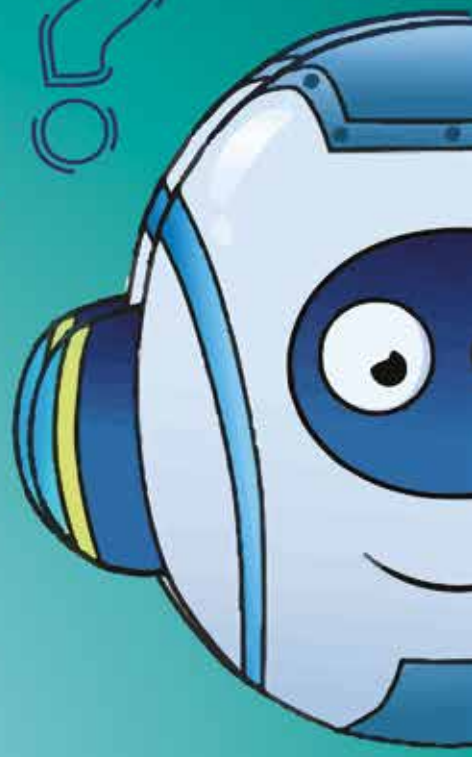
نوع من الرّوبوتات يُركّز على المهامّ المُتكرّرة ومعالجة البيانات، وغيرها من الأنشطة الرّوتينيّة التي قد تستغرق وقتًا طويلًا من البشر.

يمكن لها إرسال رسائل غير مرغوب فيها إلى الأهداف، مثل برمجيات البريد العشوائيّ، وأن تشنّ هجمات تصيُّد أو تَنْشر تعليقات سيِّئة على وسائل التَّواصل الاجتماعيّ لتشويه صورة علامة تجاريَّة أو شركة معيَّنة، وكذلك تسويق منتجات أو خدمات غير قانونيَّة.

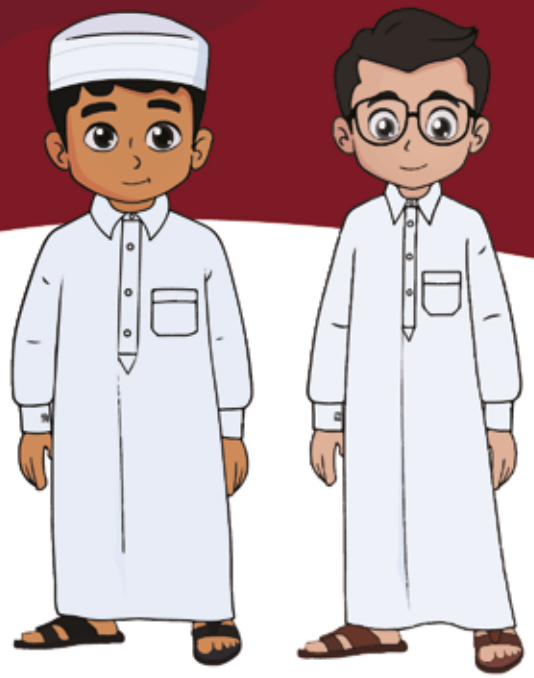
نوع من الرُّوبوتات يقوم بتثبيت برمجيَّات ضارَّة مثل الفدية والفيروسات وأحصنة طروادة والدّيدان الفيروسيَّة.

هو ملفّ موجود على خادم ويب يُوضِّح قواعد وصول الرُّوبوتات إلى الخصائص الموجودة على ذلك الخادم.

تُشير إلى حظر حركة مرور الرُّوبوتات غير المرغوب فيها أو الضَّارَّة على الإنترنت مع السَّماح للرُّوبوتات المفيدة بالوصول إلى خصائص الويب، من خلال الكشف عن نشاط الرُّوبوتات، والتَّمييز بين سلوك الرُّوبوتات المرغوب فيه وغير المرغوب فيه، وتحديد مصادر النَّشاط غير المرغوب فيه.



اخْتر الإجابة الصَّحيحة



1 - يُطلَق على روبوتات الإنترنت مسمَّيات أخرى مثل

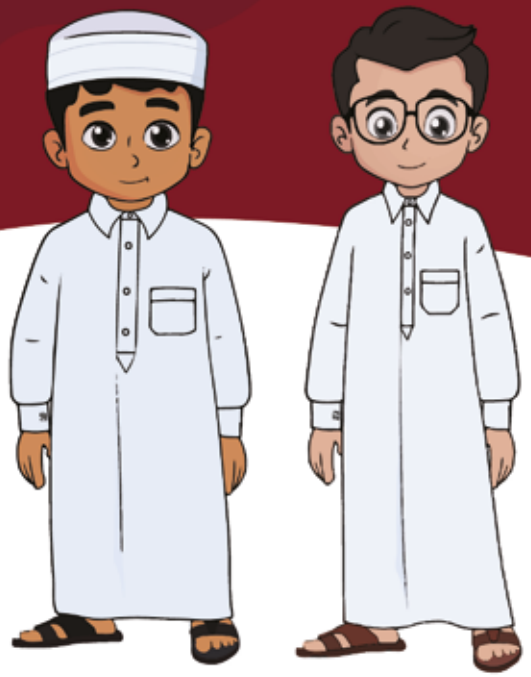
- [ ] العناكب.
- [ ] برامج الزَّحف.
- [ ] روبوتات الويب.
- [ ] جميع ما سبق.

2- تُصنَّف الرُّوبوتات بأنَّها ....

- [ ] روبوتات ضارَّة
- [ ] روبوتات نافعة.
- [ ] روبوتات محايدة.

3- إحدى الطُّرق الأكثر شيوعًا التي تُصيب بها الرُّوبوتات جهاز الحاسوب الخاصّ بك .....

- [ ] النَّسخ.
- [ ] التَّنزيل.
- [ ] النَّقل.



4- من الرُّوبوتات النَّافعة .....

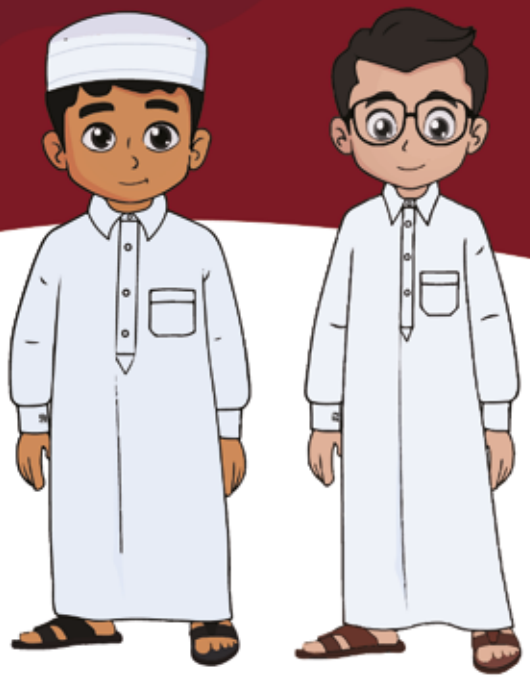
- ☐ روبوتات DDoS.
- ☐ روبوت البريد المزعج.
- ☐ روبوتات مدقّق الرَّوابط الخلفيَّة.

5- تُعْتبر الرَّوابط الخلفيَّة مهمَّة لـ

- ☐ تحسين محرّكات البحث (SEO).
- ☐ أتمتة المهامّ على منصَّات التَّواصل الاجتماعيّ.
- ☐ البحث في الإنترنت والعثور على المعلومات.

6- تُعَدّ نوعًا من برامج الدَّردشة الآليَّة التي تُوفِّر التَّوصية بالمنتجات وتساعد في شراء المنتجات .....

- ☐ روبوتات التِّجارة الإلكترونيَّة.
- ☐ روبوتات وسائل التَّواصل الاجتماعيّ.
- ☐ روبوتات الدَّردشة.



7- من أهداف إدارة الرُّوبوتات .....

- [ ] تحليل سلوك الرُّوبوت.
- [ ] إضافة برمجيّات الرُّوبوت الضَّارّة إلى القوائم المسموح بها.
- [ ] عدم الحدّ من استخدام الرُّوبوتات للخدمة بشَكْلٍ مفرطٍ.
- [ ] السَّماح بوصول الرُّوبوتات الضَّارّة إلى محتويات معيَّنة.

8- من علامات إصابة الأجهزة والملفَّات بهجوم الرُّوبوتات .....

- [ ] ارتفاع في سرعات المُعالَجة.
- [ ] عدم تعطُّل التَّطبيق بشَكْلٍ مُتكرّر.
- [ ] بُطء سرعات الإنترنت.

9- لمنع هجوم الرُّوبوتات .....

- [ ] النَّقر على جميع روابط الإنترنت.
- [ ] تنزيل جميع المرفقات البريديَّة.
- [ ] السَّماح باستخدام شبكة Wi-Fi للجميع.
- [ ] تحديث نظام التَّشغيل والبرامج الأخرى بانتظام.

كوِّن الكلمة المناسِبة من الأحرف الموجودة في الجدول

نصوص برمجيَّة ضارَّة تجتاز مواقع الويب تلقائيًّا، وتملأ نموذج الويب وتَحذِف البيانات بشَكْلٍ غير قانونيّ من مواقع الويب.

ر	ص	ي	ش	ت
م	و	غ	ال	ن
ض	ش	ب	ه	ا

تُعْرف أيضًا باسم "برامج زحف الويب"، ويتمّ استخدام هذه الرُّوبوتات للزَّحف إلى الإنترنت والعثور على المعلومات التي يحتاج إليها المَستخدِم.

م	ت	ب	ض
و	ح	ال	ث
ر	س	ك	ا

تُعْرف أيضًا باسم "روبوتات حَشْو بيانات الاعتماد"، وتستطيع الوصول إلى حسابات المُستخدِمين عن طريق شنّ هجمات من خلال استخدام أسماء المُستخدِمين وكلمات المرور المسروقة، أو خَرْق حسابات المُستخدِمين باستخدام المعلومات الحسَّاسة مثل تفاصيل بطاقة الائتمان والحساب المصرفيّ.

ر ث م ا

ك و ت و

ال ح ب س

ي ل ء ص

هو روبوت مُصمَّم لشراء منتجات أو خدمات سريعة الحركة بكمِّيَّات كبيرة، ما يجعل من الصَّعْب على العملاء الحقيقيِّين إكمال عمليَّات الشِّراء المشروعة.

ر ث م ا

ك و ت و

ال ح ب س

ي ل ء ص

هي عبارة عن روبوتات مصمَّمة لجمع المعلومات من مصادر مختلفة وإنشاء أدلَّة شاملة أو قوائم محتوى؛ لتزويد المُستخدِمين بمعلومات مُحدَّثة حول مواقع الويب أو الشَّركات أو المنتجات أو الخدمات.

ر	ن	م	ا
ك	و	ت	و
ال	ج	ب	س
ي	ل	ي	ع

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجب يقوم به الطَّالب بمفرده أو بالاشتراك مع زميل أو أكثر، ويقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

- كتَابَة قصَّة أو تقرير أو مقال يَشْرح فيه ماهيَّة روبوتات الشَّبكة العالميَّة، ويَسْتعرِض أهمّ مميِّزاتها وعيوبها.
- يَتَقَمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوْجِيهاتٍ عامَّةً لزملائه أو أَهْله يُوضِّح لهم فيها ماهيَّة روبوتات الشَّبكة العالميَّة.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency