الحاسوب

مقرر مادة الحاسوب للمرحلة الثانية

م م عمر اياد اسماعيل

مفردات ومحتويات المنهج

1- الشبكات والامن السيبراتي	2- التحول الرقمي والدفع الالكتروني	3- مقدمة الذكاء الاصطناعي	4- الذكاء الاصطناعي في حياتنا اليومية
5- تطبيقات الذكاء الاطناعي	6- الذكاء الاطناعي في المجتمع	7- تحديات الذكاء الاصطناعي	8- مستقبل الذكاء الاصطناعي

توزيع الدرجات

الامتحان النهائي من 60 درجة

السعي من 40 درجة مقمة امتحانين شهرية مع الانشطة والمشاركة والتقارير والالتزام

متطلبات عبور المادة من 50 والنجاح الحقيقي في التعلم

لمحة عامة

من الصعب اليوم تخيّل الحياة بدون أجهزة الكمبيوتر أو الأجهزة الرقمية الأخرى. في الوقت الحاضر، أصبحت معرفة كيفية استخدام الكمبيوتر حاجة ضرورية يستفيد العديد من طلابنا من الدورات الأساسية في الحاسوب التي تقدمها كليتنا، والتي تعلّمهم مبادئ الحاسوب والتقنيات والمهارات الأساسية المرتبطة بالإنترنت. نقدم في هذا المنهج أساسيات الحوسبة، بما في ذلك استخدام مجموعة متنوعة من مكونات الأجهزة والبرمجيات. ولا يشترط وجود معرفة مسبقة في البرمجة أو علوم الحاسوب.

الاهداف

تهدف هذه السنة الدراسية إلى إكساب الطلاب المعرفة الأساسية في مجال الشبكات والأمن السيبراني، وفهم مفاهيم التحول الرقمي والدفع الإلكتروني، بالإضافة إلى بناء قاعدة معرفية في الذكاء الاصطناعي. كما تهدف إلى تطوير وعي الطلاب بتطبيقات الذكاء الاصطناعي في الحياة اليومية والمجتمع، وتعزيز قدرتهم على تحليل التحديات المرتبطة به، مع استشراف مستقبل الذكاء الاصطناعي ودوره في العالم الحديث.

الشبكات

مقدمة عن شبكات الحاسوب

شبكات الحاسوب تمكِّن المستخدمين من:

- إرسال الرسائل (نصوص، صور، أصوات...) لعدة أشخاص دفعة واحدة.
- الاتصال ببنوك المعلومات والمكتبات العالمية من أي مكان.
- عقد مؤتمرات وندوات عن بعد.
- استخدام التعليم والطب والتجارة والحكومة الإلكترونية.
- **ما هي شبكة الحاسوب؟**

هي مجموعة من الحاسبات والأجهزة المتصلة ببعضها بهدف مشاركة البيانات والبرمجيات والأجهزة، وتُعتبر وسيلة اتصال إلكترونية بين الأفراد.

فوائد الشبكة

- المشاركة في الأجهزة: مثل الطابعات.
- المشاركة في البرمجيات: مثل البريد الإلكتروني والملفات.
- المشاركة في البيانات: مثل قواعد بيانات البنوك وتذاكر السفر.
- توفير في التكاليف دعم اتخاذ القرار.التجارة الإلكترونية.الخدمات الحكومية الرقمية.

اجهزة الشبكة

- **الخادم:(Server)**

جهاز مركزي عالي الكفاءة يخزن البيانات والبرامج ويتحكم في إدارة الشبكة وخدماتها.

- **محطات العمل:(Workstations)**

أجهزة يستخدمها الأفراد للتفاعل مع الشبكة والاستفادة من مواردها.

- **خطوط الاتصال:(Communication Lines)**

الوسائط التي يتم عبرها تبادل البيانات بين الأجهزة (سلكية أو لاسلكية).

- **بطاقة الشبكة:(NIC)**

قطعة إلكترونية تُمكّن الحاسوب من الاتصال بالشبكة.

- **المودم:(Modem)**

جهاز يحوّل الإشارات بين الحاسوب وخط الهاتف لتوصيله بالإنترنت.

- **الأجهزة الملحقة:**

أدوات إضافية تُربط بالشبكة مثل الطابعات وأجهزة الفاكس ليستفيد منها جميع المستخدمين.

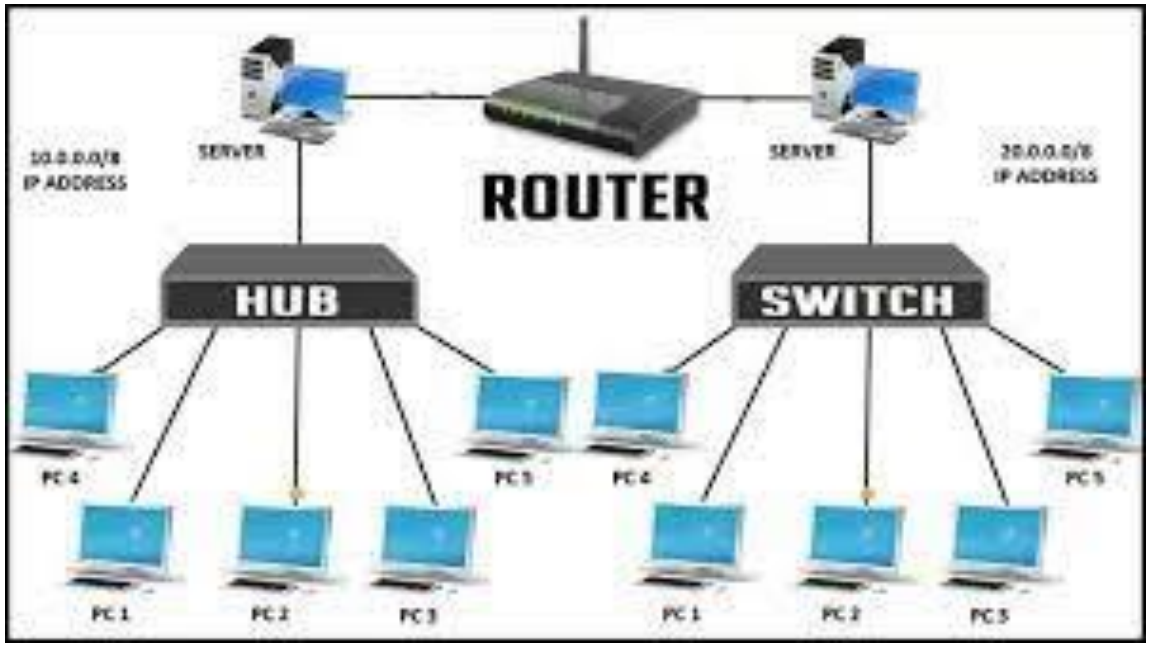
- **محولات الشبكة:(Switches)**

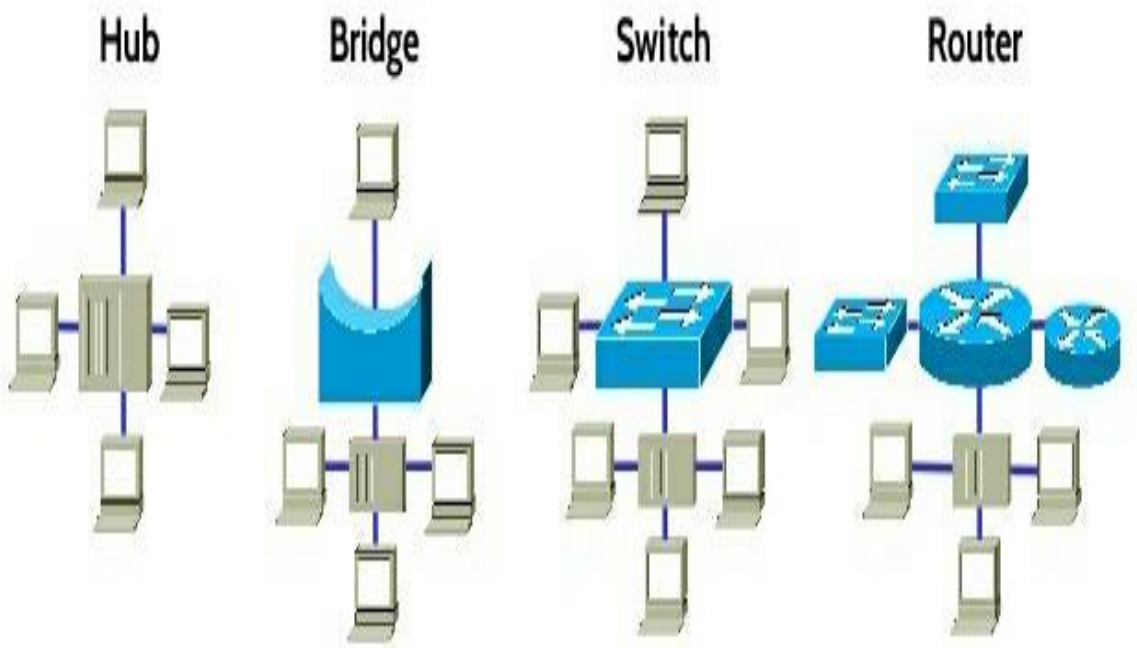
أجهزة تنظم حركة البيانات بين الأجهزة وتربط الشبكات معًا (مثل الجسر، الموزع، البوابة، الموجه).

- **برامج الشبكة:**

برمجيات تُدير الشبكة وتتحكم في كيفية تبادل البيانات بين الأجهزة.

اجهزة الشبكة

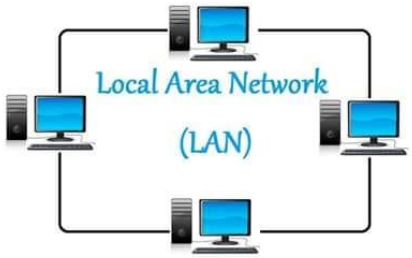




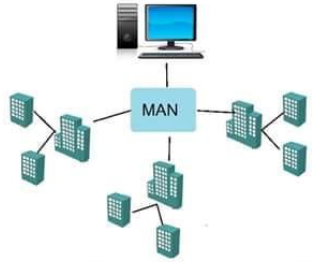
انواع الشبكات حسب الحجم

1. **الشبكة المحلية :LAN** تربط أجهزة في منطقة جغرافية قريبة (مكتب – مدرسة).
2. **الشبكة الواسعة :WAN** تربط أجهزة أو شبكات محلية على مسافات كبيرة (مدن – دول).
3. **الإنترانت :Intranet** شبكة داخلية بمؤسسة تعتمد على تقنيات الإنترنت.
4. **الإكسترانت :Extranet** تسمح لأشخاص مخولين بالدخول دون الإخلال بخصوصية الإنترانت.
5. **الإنترنت :Internet** الشبكة العالمية التي تصل بين ملايين الأجهزة حول العالم.

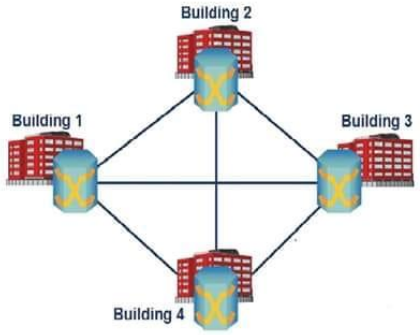
انواع الشبكات حسب الحجم



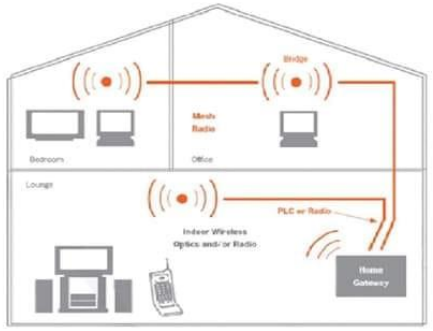
(WAN) Wide Area Network



Metropolitan Area Network



Campus Area Network(CAN)

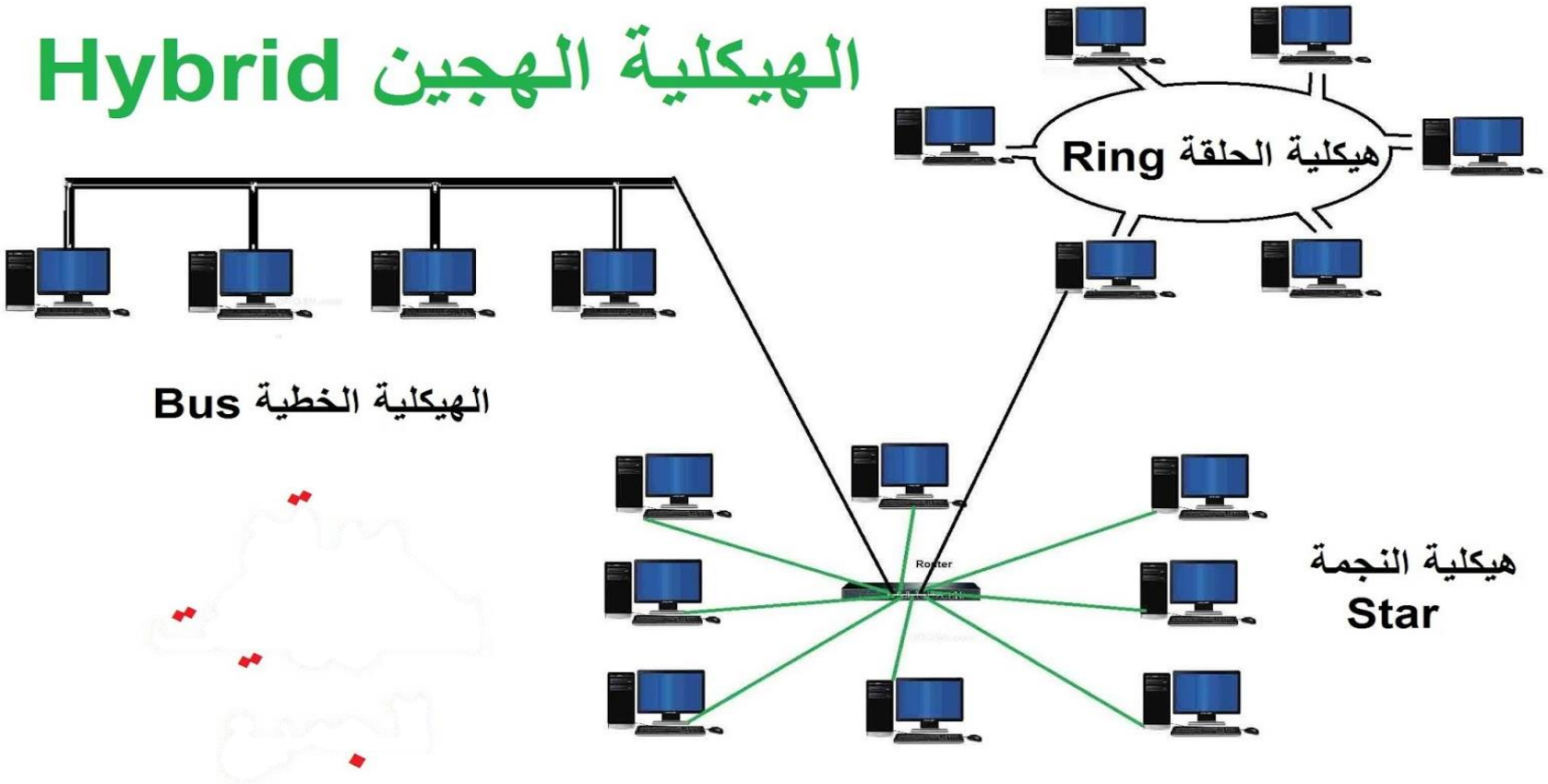


Home Area Network(HAN)

انواع الشبكات حسب طريقة الربط

- **الشبكة الخطية Bus:** كابل محوري واحد تتصل به جميع الأجهزة.
- **الشبكة الحلقية Ring:** البيانات تدور في اتجاه واحد داخل حلقة.
- **الشبكة النجمية Star:** كل جهاز متصل بالحاسوب الرئيسي فقط.

انواع الشبكات حسب طريقة الربط



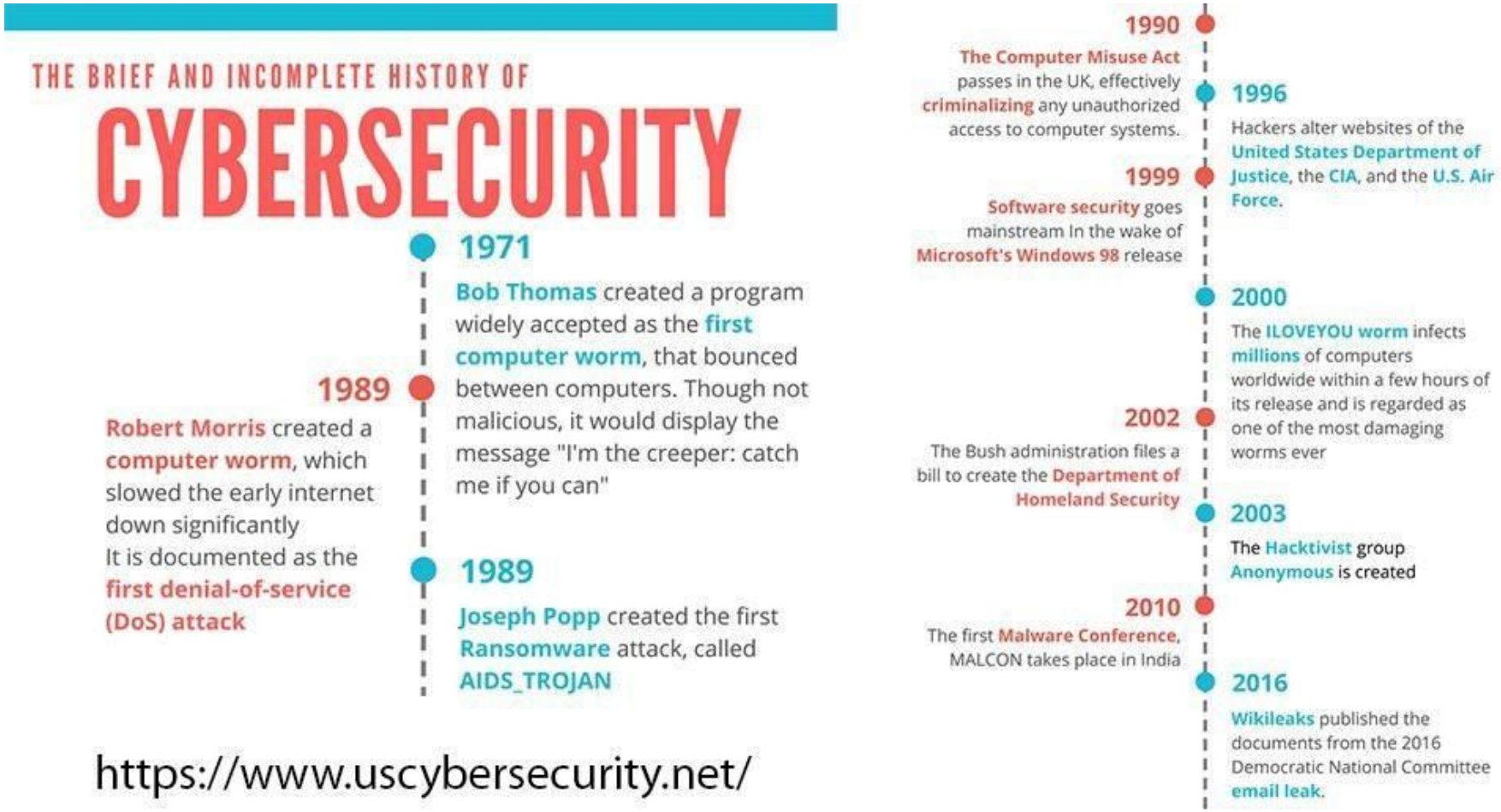
انواع الشبكات حسب طريقة الربط

- **الشبكة الخطية Bus:** كابل محوري واحد تتصل به جميع الأجهزة.
- **الشبكة الحلقية Ring:** البيانات تدور في اتجاه واحد داخل حلقة.
- **الشبكة النجمية Star:** كل جهاز متصل بالحاسوب الرئيسي فقط.

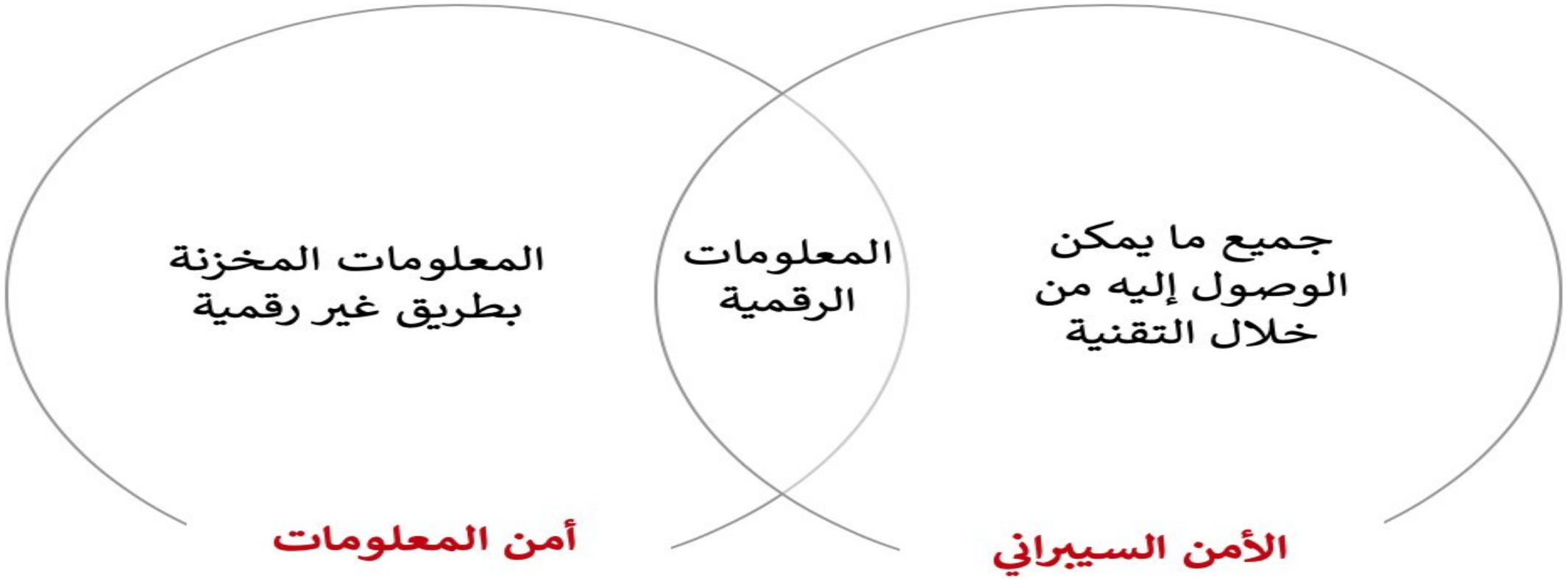
الأمن السيبراني

- الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية.
- تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية.
- يمثل تنفيذ تدابير الأمن السيبراني اليوم تحديًا كبيرًا نظرًا لوجود عدد أجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكارًا.

متى نشأ الامن السيبراني ؟



الفرق بين أمن المعلومات والأمن السيبراني




مثلث الحماية
CIA Triad
سلامة المحتوى
التأكد من أنه لم يتم التعديل
على البيانات
سواء بالحذف او الإضافه
INTEGRITY
AVAILABILITY
INFORMATION SECURITY
CONFIDENTIALITY
التوافر
إتاحة الوصول إلى البيانات
من الأشخاص المصرح لهم
السرية
حماية البيانات من الإطلاع عليها بدون صلاحية
Researchers

ما هو الأمن السيبراني

- الهدف من تنفيذ الأمن السيبراني، هو توفير وضع أمني جيد لأجهزة الكمبيوتر والخوادم والشبكات والأجهزة المحمولة والبيانات المخزنة على هذه الأجهزة من المهاجمين ذوي النوايا الخبيثة،
- ان الهدف من تصميم الهجمات الإلكترونية هي للوصول إلى البيانات الحساسة للمؤسسة أو المستخدم أو حذفها أو ابتزازها. لذلك فان الجميع الآن في حاجة إلى وجود الأمن السيبراني سواء في المؤسسات والشركات والمصانع والجهات الحكومية وحتى المنازل.

أهمية الأمن السيبراني

- يعد الأمن السيبراني مهماً لأن الموسسات الحكومية والعسكرية والشركات والمالية والطبية تجمع وتعالج وتخزن كميات غير مسبوقة من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى.
- تنقل الموسسات البيانات الحساسة عبر الشبكات والأجهزة الأخرى أثناء ممارسة الأعمال التجارية، ويوصف الأمن السيبراني ان هو النظام المخصص لحماية تلك المعلومات والأنظمة المستخدمة لمعالجتها أو تخزينها.
- مع نمو حجم وتعقيد الهجمات الإلكترونية، يتعين على الشركات والمؤسسات وخاصة تلك المكلفة بحماية المعلومات المتعلقة بالأمن القومي أو الصحة أو السجلات المالية، اتخاذ خطوات لحماية معلومات الأعمال والموظفين الخاصة بهم.
- في مارس 2013، حذرمن أن الهجمات الإلكترونية والتجسس الرقمي تشكل أكبر تهديد للأمن لاي بلد وتتفوق حتى على الإرهاب.

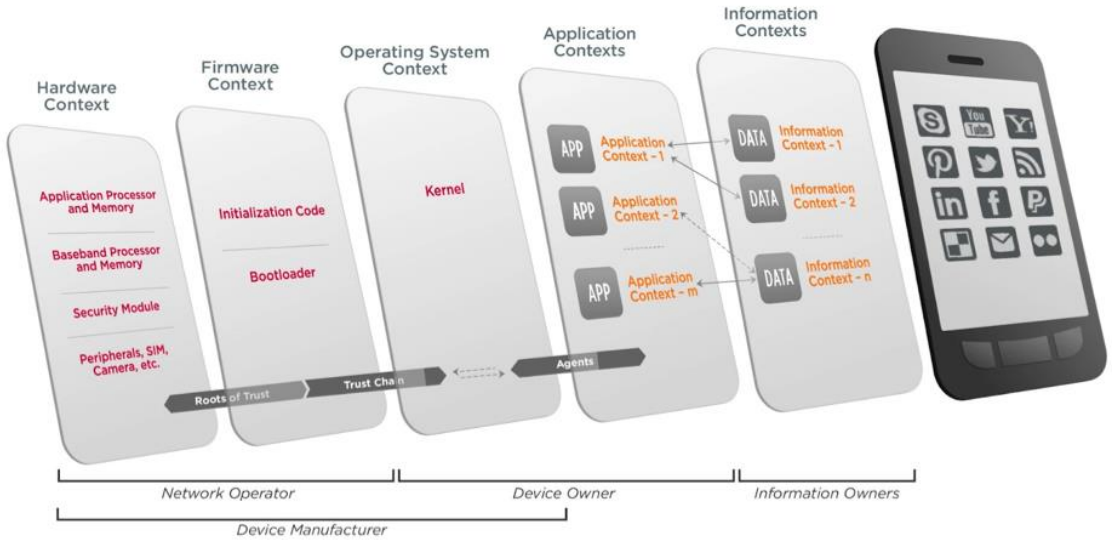
تحديات الأمن السيبراني

للحصول على أمن إلكتروني فعال، تحتاج الموسسة إلى تنسيق جهودها في جميع أنحاء نظام المعلومات الخاص بها، وتشمل عناصر الإنترنت كل ما يلي:

- **أمن الشبكة:** عملية حماية الشبكة من المستخدمين غير المرغوب فيهم والهجمات والاقتحامات.
- **أمان التطبيق:** تتطلب التطبيقات تحديثات واختبارات مستمرة للتأكد من أن هذه البرامج آمنة من الهجمات.
- **أمان نقطة النهاية:** يعد الوصول عن بُعد جزءاً ضرورياً من العمل، ولكنه قد يكون أيضاً نقطة ضعف للبيانات، أمان نقطة النهاية هو عملية حماية الوصول عن بُعد إلى شبكة الشركة.
- **أمن البيانات:** توجد بيانات داخل الشبكات والتطبيقات، تعد حماية معلومات الشركة والعملاء طبقة منفصلة من الأمان.
- **إدارة الهوية:** هذه هي عملية فهم الوصول الذي يتمتع به كل فرد في المؤسسة.
- **قاعدة البيانات وأمن البنية التحتية:** كل شيء في الشبكة يتضمن قواعد بيانات ومعدات مادية، حماية هذه الأجهزة لا تقل أهمية.
- **أمان السحابة:** توجد العديد من الملفات في البيئات الرقمية أو «السحابة»، تمثل حماية البيانات في بيئة عبر الإنترنت بنسبة 100% قدراً كبيراً من التحديات.

تحديات الأمن السيبراني

- **أمان الأجهزة المحمولة:** تشتمل الهواتف المحمولة والأجهزة اللوحية تقريباً على كل نوع من التحديات الأمنية في حد ذاتها.
- **التعافي من الكوارث والتخطيط لاستمرارية الأعمال:** في حالة حدوث خرق، يجب حماية بيانات الكوارث الطبيعية أو غيرها من بيانات الأحداث ويجب أن يستمر العمل، ولهذا ستحتاج إلى خطة.
- **تعليم المستخدم النهائي:** قد يكون المستخدمون موظفين يصلون إلى الشبكة أو عملاء يسجلون الدخول إلى تطبيق الشركة، ويعد تعليم العادات الجيدة (تغيير كلمة المرور، والمصادقة الثنائية، وما إلى ذلك) جزءاً مهماً من الأمن السيبراني.



ان التحدي الأكثر صعوبة في الأمن السيبراني هو الطبيعة المتطورة باستمرار للمخاطر الأمنية نفسها، حيث ركزت المؤسسات والحكومات على معظم موارد الأمن السيبراني على الأمن المحيط لحماية مكونات النظام الأكثر أهمية والدفاع ضد المعالجات المعروفة. اليوم هذا النهج أصبح غير كافٍ، حيث تتقدم التهديدات وتتغير بسرعة أكبر مما تستطيع المؤسسات مواكبة ذلك، نتيجة لذلك تعمل المؤسسات الاستشارية على تعزيز أساليب أكثر استباقية وتكيفاً للأمن السيبراني، وقد أصدر المعهد الوطني للمعايير والتكنولوجيا NIST إرشادات في إطار تقييم المخاطر الخاص به والتي توصي بالتحول نحو المراقبة المستمرة والتقييمات في الوقت الفعلي، وهو نهج يركز على البيانات للأمن بدلاً من النموذج التقليدي القائم على المحيط.

أنواع التهديدات الإلكترونية للأمن السيبراني

تأتي الهجمات الإلكترونية بجميع الأشكال والأحجام، قد يكون بعضها عبارة عن هجمات برامج الفدية العلنية (اختطاف منتجات أو أدوات تجارية مهمة مقابل الحصول على أموال مقابل إطلاقها)، في حين أن بعضها عبارة عن عمليات سرية يتسلل من خلالها المجرمون إلى نظام للحصول على بيانات قيمة فقط ليتم اكتشافها بعد أشهر من وقوعها. يزداد المجرمون براعة في أعمالهم الخبيثة، وهنا بعض الأنواع الأساسية للهجمات الإلكترونية التي تؤثر على آلاف الأشخاص كل يوم.

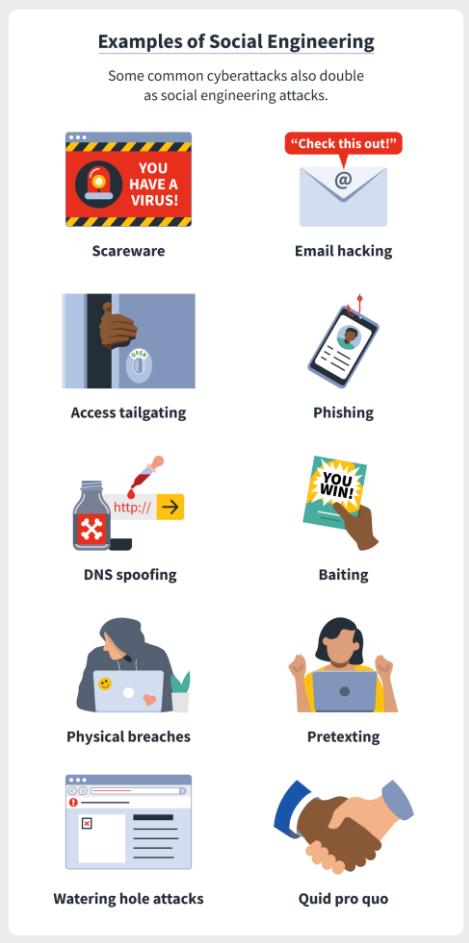
1.البرمجيات الخبيثة

- تستخدم «البرامج الخبيثة»Malware لوصف البرامج الضارة بما في ذلك برامج التجسس وبرامج الفدية والفيروسات، عادة ما تخترق الشبكات من خلال ثغرة أمنية، مثل النقر على روابط البريد الإلكتروني المشبوهة أو تثبيت تطبيق محفوف بالمخاطر. بمجرد الدخول إلى الشبكة، يمكن للبرامج الخبيثة الحصول على معلومات حساسة، وإنتاج المزيد من البرامج الضارة في جميع أنحاء النظام، ويمكنها أيضاً حظر الوصول إلى مكونات شبكة الأعمال الحيوية (برامج الفدية).

2.التصيد

- التصيد Phishing الاحتيالي هو ممارسة إرسال اتصالات ضارة (عادةً رسائل بريد إلكتروني) مصممة لتظهر من مصادر حسنة السمعة ومعروفة، تستخدم رسائل البريد الإلكتروني هذه الأسماء والشعارات والصياغة وما إلى ذلك، كشركة لتقليل الشكوك وجعل الضحايا ينقرون على الروابط الضارة. بمجرد النقر فوق ارتباط التصيد، يمكن لمجرمي الإنترنت الوصول إلى البيانات الحساسة مثل بطاقة الائتمان أو الضمان الاجتماعي أو معلومات تسجيل الدخول.

أنواع التهديدات الإلكترونية للأمن السيبراني

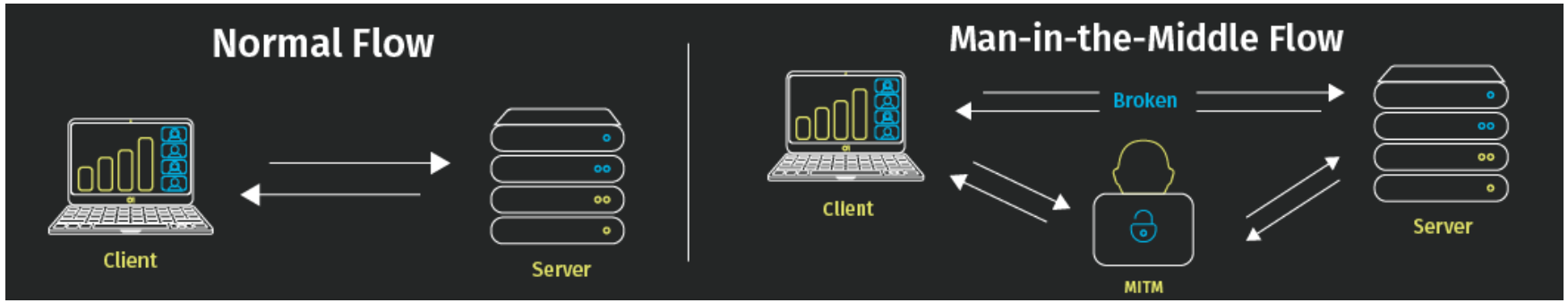


3.هندسة اجتماعية

- الهندسة الاجتماعية هي عملية التلاعب النفسي بالناس لإفشاء معلومات شخصية، التصيد هو شكل من أشكال الهندسة الاجتماعية، حيث يستغل المجرمون فضول الناس الطبيعي أو ثقتهم. يعد التلاعب بالصوت أحد الأمثلة على الهندسة الاجتماعية الأكثر تقدماً، في هذه الحالة يأخذ مجرمو الإنترنت صوت الفرد (من مصادر مثل البريد الصوتي أو منشور على وسائل التواصل الاجتماعي) ويتلاعبون به للاتصال بالأصدقاء أو الأقارب وطلب بطاقة ائتمان أو معلومات شخصية أخرى.

4.هجوم MitM

- تحدث هجمات Man-in-the-Middle (MitM)عندما يقطع المجرمون حركة المرور بين المعاملات بين طرفين، على سبيل المثال: يمكن للمجرمين إدخال أنفسهم بين شبكة Wi-Fiعامة وجهاز الفرد، بدون اتصال Wi-Fiمحمي، يمكن لمجرمي الإنترنت أحياناً عرض جميع معلومات الضحية دون أن يتم القبض عليهم.



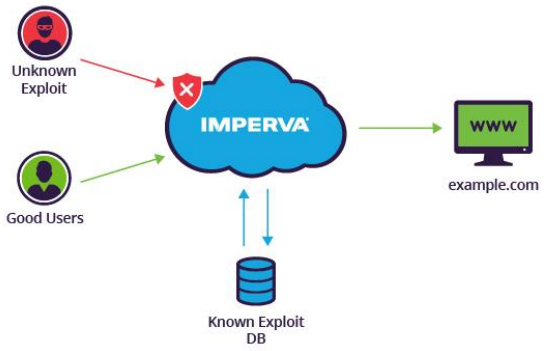
أنواع التهديدات الإلكترونية للأمن السيبراني

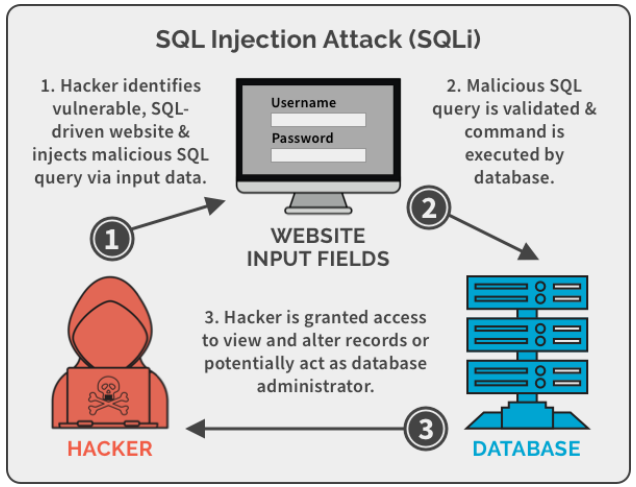
5.هجوم Zero-day

- أصبحت هجمات Zero-dayأكثر شيوعاً، تحدث هذه الهجمات بين إعلان ثغرة أمنية في الشبكة وحل التصحيح، باسم الشفافية والأمان، ستعلن معظم الشركات أنها وجدت مشكلة في أمان شبكتها، لكن بعض المجرمين سيغتنمون هذه الفرصة لشن هجمات قبل أن تتمكن الشركة من التوصل إلى تصحيح أمني.

6. لغة الاستعلام الهيكلية SQL

- يعمل هذا التهديد عن طريق إدخال تعليمات برمجية ضارة في نموذج على موقع الويب أو التطبيق الخاص بالشركة، ما يسمح للمهاجم بالكشف عن المعلومات الحساسة.





أساسيات الأمن السيبراني لإحباط الهجمات الإلكترونية

- يعد نهج الأمن السيبراني متعدد الطبقات هو أفضل طريقة لإحباط أي هجوم إلكتروني خطير، ستساعد مجموعة من جدران الحماية والبرامج ومجموعة متنوعة من الأدوات في مكافحة البرامج الضارة التي يمكن أن تؤثر على كل شيء من الهواتف المحمولة إلى شبكة Wi-Fi، في ما يلي بعض الطرق التي يقاوم بها خبراء الأمن السيبراني إيقاف الهجمات الرقمية.

أساسيات الأمن السيبراني لإحباط الهجمات الإلكترونية

1.الذكاء الاصطناعي للأمن السيبراني

يتم استخدام الذكاء الاصطناعي في الأمن السيبراني لإحباط مجموعة واسعة من الجرائم الإلكترونية الخبيثة، تقوم شركات الأمن بتدريب أدوات الذكاء الاصطناعي للتنبؤ بانتهاكات البيانات، والتنبيه لمحاولات التصيد في الوقت الفعلي وحتى فضح عمليات الاحتيال في الهندسة الاجتماعية قبل أن تصبح خطيرة.

2.تأمين ضد البرامج الضارة

يعد الأمان ضد البرامج الضارة بالتأكيد، أحد أهم مشكلات اليوم (وسيظل كذلك مع تطور البرامج الضارة)، هناك حاجة إلى حزمة برامج مكافحة الفيروسات لمكافحة أي نشاط مشبوه، تتضمن هذه الحزم عادةً أدوات تقوم بكل شيء بدءاً من التحذير من المواقع المشبوهة وحتى الإبلاغ عن رسائل البريد الإلكتروني التي قد تكون ضارة.

أساسيات الأمن السيبراني لإحباط الهجمات الإلكترونية

3. امن الهاتف

الهواتف المحمولة هي واحدة من أكثر الأجهزة المعرضة لخطر الهجمات السيبرانية والتهديد آخذ في الازدياد. يعد فقدان الجهاز الشاغل الأكبر بين خبراء الأمن السيبراني.

قد يكون ترك هواتفنا في مطعم أو حتى سرقته أمراً خطيراً، لحسن الحظ هناك أدوات تقفل جميع استخدامات الهواتف المحمولة (أو تسن كلمات مرور متعددة العوامل) في حالة حدوث هذا الحادث.

أصبح أمان التطبيق أيضاً مشكلة رئيسية أخرى، لمكافحة تطبيقات الأجهزة المحمولة التي تتطلب الكثير من الامتيازات أو إدخال فيروسات أحصنة طروادة أو تسريب معلومات شخصية، يلجأ الخبراء إلى أدوات الأمن السيبراني التي ستنبه الأنشطة المشبوهة أو تحظرها تماماً.

أساسيات الأمن السيبراني لإحباط الهجمات الإلكترونية

4. أمان مستعرض الويب والسحابة

- أمان المستعرض هو تطبيق لحماية البيانات المتصلة بالإنترنت والمتصلة بالشبكة من انتهاكات الخصوصية أو البرامج الضارة، تشتمل أدوات متصفح مكافحة الفيروسات على أدوات منع النوافذ المنبثقة والتي تنبه ببساطة أو تحظر الروابط والإعلانات غير المرغوب فيها والمريبة.
- تتضمن التكتيكات الأكثر تقدماً المصادقة الثنائية، واستخدام المكونات الإضافية للمستعرض التي تركز على الأمان واستخدام المتصفحات المشفرة.

5. أمان Wi-Fi

- يمكن أن يجعلك استخدام شبكة Wi-Fi العامة عرضة لمجموعة متنوعة من الهجمات الإلكترونية عبر الإنترنت. للحماية من هذه الهجمات، يقترح معظم خبراء الأمن السيبراني استخدام أحدث البرامج، وتجنب المواقع المحمية بكلمة مرور والتي تحتوي على معلومات شخصية (البنوك ووسائل التواصل الاجتماعي والبريد الإلكتروني وما إلى ذلك).
- الطريقة الأكثر أماناً للحماية من هجوم إلكتروني على شبكة Wi-Fi العامة هي استخدام شبكة افتراضية خاصة (VPN)، تنشئ شبكات VPN شبكة آمنة، حيث يتم تشفير جميع البيانات المرسلة عبر اتصال Wi-Fi.

6. تعليم المستخدم

- يتضمن تعليم المستخدم النهائي تعليم المستخدمين اتباع أفضل الممارسات مثل عدم النقر على روابط غير معروفة أو تنزيل مرفقات مشبوهة في رسائل البريد الإلكتروني، ما قد يسمح بدخول البرامج الضارة وأشكال أخرى من البرامج الضارة.

الفرق بين الأمن السيبر اني وأمن الكمبيوتروأمن تكنولوجيا المعلومات

الفرق بين الأمن السيبر اني وأمن الكمبيوتروأمن تكنولوجيا المعلومات

كما ذكر أعلاه، فإن الأمن السيبراني هو ممارسة للدفاع عن الأنظمة الإلكترونية والشبكات وأجهزة الكمبيوتر والأجهزة المحمولة والبرامج والبيانات من الهجمات الرقمية الضارة. يمكن لمجرمي الإنترنت نشر مجموعة متنوعة من الهجمات ضد الضحايا الأفراد أو الشركات التي يمكن أن تشمل الوصول إلى البيانات الحساسة أو تغييرها أو حذفها، دفع ابتزاز أو التدخل في العمليات التجارية. يتم تحقيق الأمن السيبراني، من خلال بنية تحتية مقسمة على 3 مكونات رئيسية (أمن تكنولوجيا المعلومات، والأمن السيبراني، وأمن الكمبيوتر).

أمن تكنولوجيا المعلومات : IT

هو حماية البيانات في كل من مكان تخزينها وأثناء التنقل عبر الشبكة، بينما يحمي الأمن السيبراني البيانات الرقمية فقط، فإن أمن تكنولوجيا المعلومات يحمي البيانات الرقمية والمادية من المتطفلين.

الأمن السيبر اني:

هو مجموعة فرعية من أمن تكنولوجيا المعلومات، بينما يحمي أمن تكنولوجيا المعلومات كل من البيانات المادية والرقمية، فإن الأمن السيبر اني يحمي البيانات الرقمية على شبكاتك وأجهزة الكمبيوتر والأجهزة الخاصة بك من الوصول غير المصرح به والهجوم والتدمير.

أمان الشبكة أو أمان الكمبيوتر:

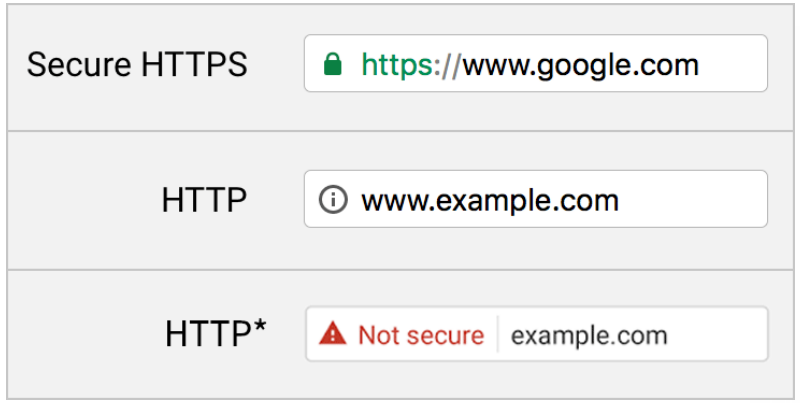
هو مجموعة فرعية من الأمن السيبراني، يستخدم هذا النوع من الأمان، الأجهزة والبرامج لحماية أي بيانات يتم إرسالها عبر جهاز الكمبيوتر الخاص بك والأجهزة الأخرى إلى الشبكة. يعمل أمان الشبكة على حماية البنية التحتية لتكنولوجيا المعلومات والحماية من المعلومات التي يتم اعتراضها وتغييرها أو سرقتها من قبل مجرمي الإنترنت.

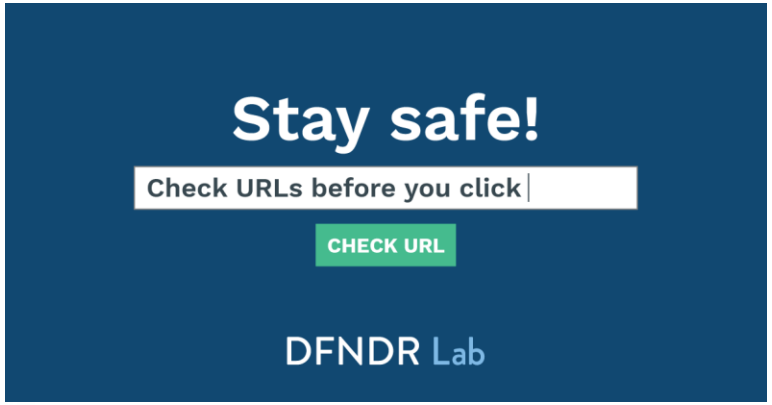
نصائح للمستخدمين عن للأمن السيبراني

أصبح الإنترنت فضاءً مليئاً بالروابط الخبيثة والفيروسات، أصبحت خروقات البيانات أكثر تواتراً، وأصبح المستخدمون غير المرتابين أكثر عرضة للخطر من أي وقت مضى. عندما تكلف نقرة واحدة الآلاف، بل وحتى الملايين، يحتاج المستخدمون إلى مهام قابلة للتنفيذ يمكن أن تساعدهم في البقاء في حالة تأهب وأمان عبر الإنترنت. فيما يلي أهم نصائح للأمن السيبراني للمستخدمين:

النقر بدون تفكير

فقط لأنك تستطيع النقر، لا يعني أنه يجب عليك ذلك، تذكر يمكن أن يكلفك ذلك مبلغاً ضخماً، يمكن أن تلحق الروابط الضارة بعدة طرق مختلفة، لذا تأكد من فحص الروابط والتأكد من أنها من مرسلين موثوق بهم قبل النقر عليها





نصائح للمستخدمين عن للأمن السيبراني

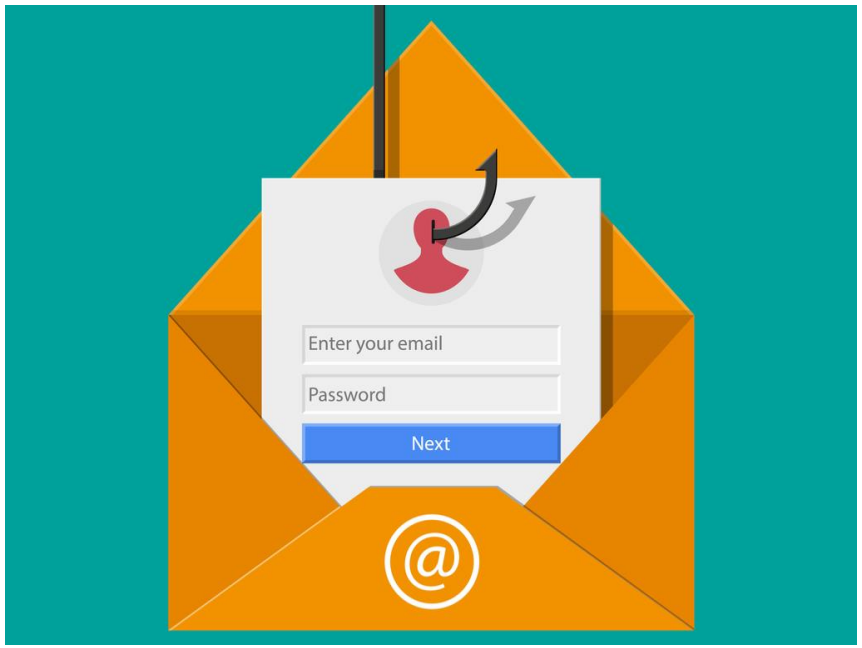
استخدم المصادقة الثنائية

من المهم أن تكون لديك كلمة مرور قوية، ولكن من الضروري أن تكون لديك مصادقة ثنائية أو متعددة العوامل، توفر هذه الطريقة طبقتين من إجراءات الأمان، لذلك إذا تمكن المتسلل من تخمين كلمة مرورك بدقة، فلا يزال هناك إجراء أمني إضافي مطبق لضمان عدم اختراق حسابك.

نصائح للمستخدمين عن للأمن السيبراني

ابحث عن رسائل التصيد الاحتيالي

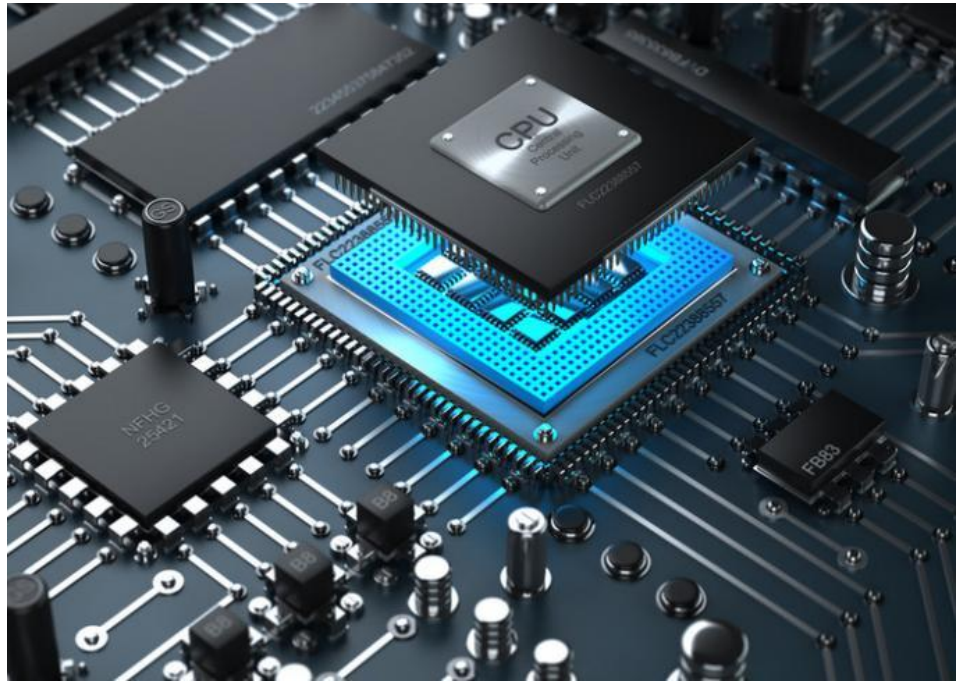
مع إرسال أكثر من 3 مليارات رسالة بريد إلكتروني مزيفة يومياً، تعد هجمات التصيد الاحتيالي من أعظم تهديدات الأمن السيبراني، حيث من السهل جداً الوقوع فيها. في هجوم التصيد الاحتيالي، سيظهر المتسلل كشخص قد يكون المتلقي مألوفاً له لخداعه لفتح رابط ضار، أو الكشف عن بيانات اعتماد مهمة، أو فتح برنامج يصيب نظام المستلم بفيروس. أفضل طريقة للبحث عن حيل التصيد الاحتيالي هي تجنب رسائل البريد الإلكتروني من مرسلين غير مألوفين، والبحث عن الأخطاء النحوية أو أي تناقضات في البريد الإلكتروني تبدو مريبة، وتحوم فوق أي رابط تتلقاه للتحقق من الوجهة.

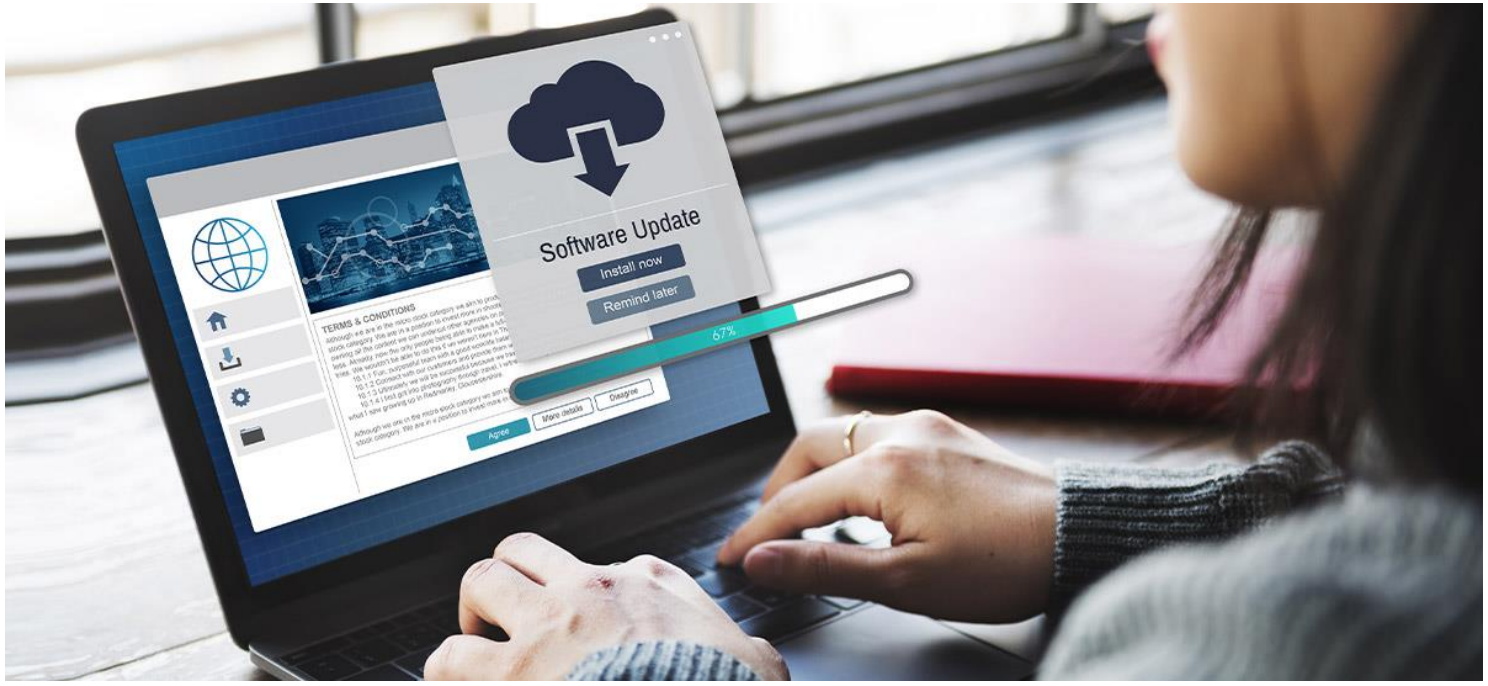


نصائح للمستخدمين عن للأمن السيبراني

مواكبة التحديثات

يمكن إصدار تصحيحات البرامج عند اكتشاف ثغرات أمنية. إذا وجدت أن إعلانات تحديث البرامج هذه مزعجة، فأنت لست وحدك، لذلك يجب التقييم وإعادة تشغيل جهازك مقابل تعريض نفسك لخطر البرامج الضارة وأنواع أخرى من عدوى الكمبيوتر.





نصائح للمستخدمين عن للأمن السيبراني

الاتصال بأمان

الالتزام بنصائح الأمن السيبراني التي تصدر من قبل الخبير التقني، لكن لا يزال الكثيرون لا يتبعون هذه النصيحة، قد تميل إلى توصيل جهازك باتصال غير آمن، ولكن عندما تزن العواقب، فإن الأمر لا يستحق ذلك، اتصل فقط بالشبكات الخاصة عندما يكون ذلك ممكناً، خاصة عند التعامل مع المعلومات الحساسة.

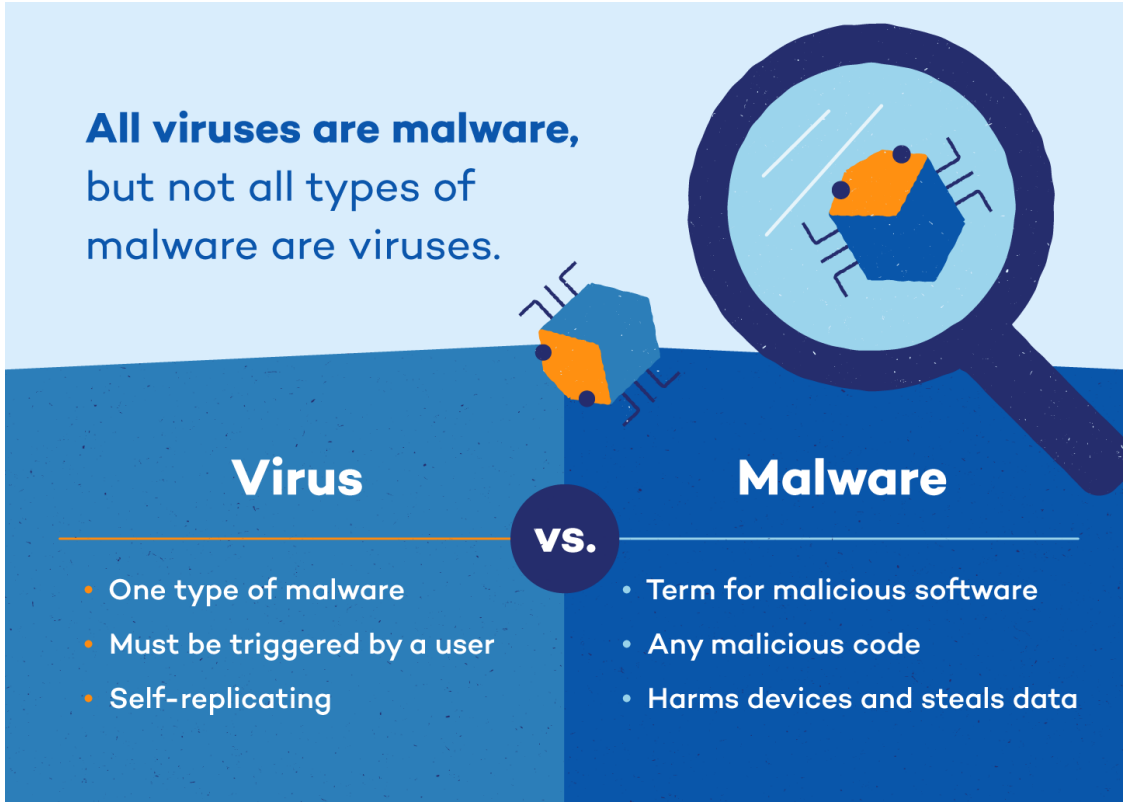
نصائح للمستخدمين عن للأمن السيبراني

تتبع البصمة الرقمية الخاصة بك

عندما تراقب حساباتك، يمكنك التأكد من ضبط نشاط مريب، هل يمكنك أن تتذكر كل مكان لديك حسابات عبر الإنترنت وما هي المعلومات المخزنة عليها مثل أرقام بطاقات الائتمان لتسهيل عمليات الدفع؟ من المهم تتبع بصمتك الرقمية، بما في ذلك وسائل التواصل الاجتماعي، وحذف الحسابات التي لا تستخدمها، مع التأكد من تعيين كلمات مرور قوية (تقوم بتغييرها بانتظام).

نصائح للمستخدمين عن للأمن السيبراني

استخدم برامج مكافحة الفيروسات والبرامج الضارة

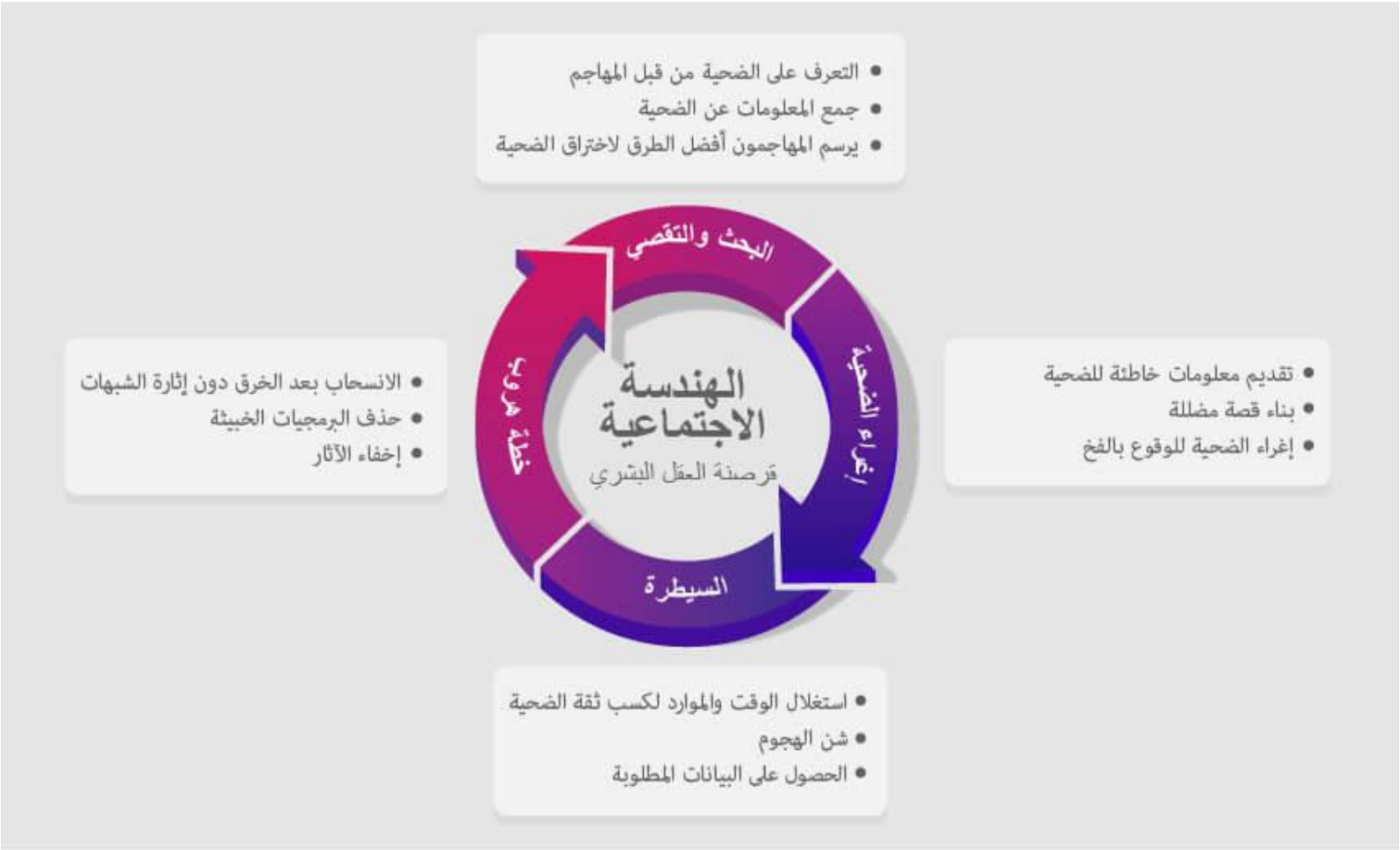


نصائح للمستخدمين عن للأمن السيبراني

تأمين جهازك المحمول

الأمن لا ينتهي عند سطح مكتبك، من المهم التعود على عادة تأمين وجودك من خلال جهازك المحمول أيضاً، استخدم كلمات مرور قوية، وتأكد من إيقاف تشغيل Bluetooth، وعدم الاتصال تلقائياً بأي شبكة Wi-Fi عامة، وقم بالتنزيل بحذر.

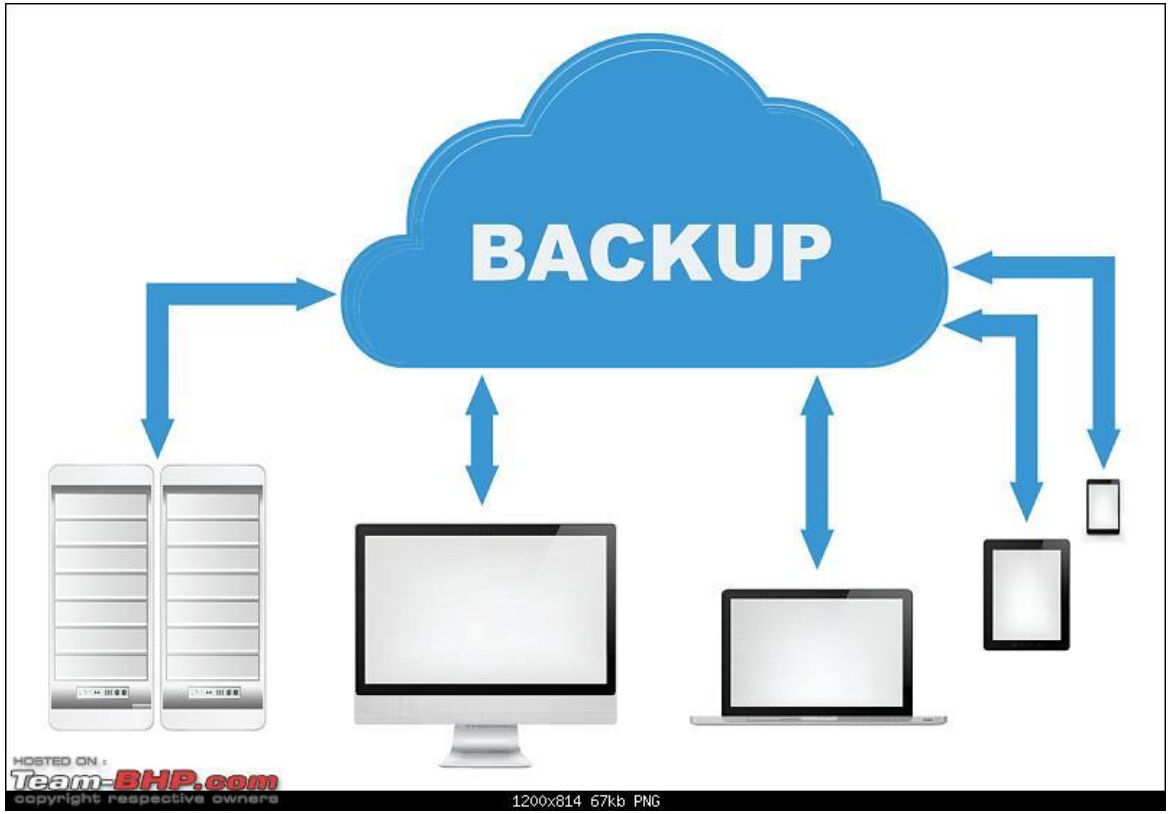
نصائح للمستخدمين عن للأمن السيبراني



احذر من الهندسة الاجتماعية

عندما لا يتمكن المتسللون من العثور على ثغرة أمنية، فإنهم سيهاجمون بطرق أخرى، هذا النوع من الهجوم هو هجوم على عقل المستخدم، وليس على الجهاز للوصول إلى الأنظمة والمعلومات، خاصة مع المعلومات المتاحة للجمهور عبر الإنترنت وعبر وسائل التواصل الاجتماعي، يبتكر مجرمي الإنترنت طرقاً مبتكرة لخداع المستخدمين.

نصائح للمستخدمين عن للأمن السيبراني



النسخ الاحتياطي لبياناتك

في هذه الأيام، لا يكلف التخزين كثيراً، ليس هناك عذر لعدم الحصول على نسخة احتياطية من البيانات المهمة، انسخه احتياطياً في موقع فعلي وعلى السحابة. تذكر أن التهديدات الخبيثة والمتسللين لا يريدون دائماً سرقة بياناتك، ولكن في بعض الأحيان يكون الهدف النهائي هو تشفيرها أو محوها، قم بعمل نسخة احتياطية للحصول على أداة استرداد نهائية.

نصائح للمستخدمين عن للأمن السيبراني

لا تكن كسولًا بشأن كلمات مرورك!

Top 10 Worst Passwords - Historic Analysis

	2021	2015	2010	2005	2000
#1	123456	123456	123456	password	password
#2	123456789	password	password	123456	123456
#3	qwerty	12345	12345678	12345678	12345678
#4	password	12345678	qwerty	abc123	qwerty
#5	1234567	qwerty	abc123	qwerty	abc123
#6	12345678	1234567890	123456789	monkey	monkey
#7	12345	1234	111111	letmein	1234567
#8	iloveyou	baseball	1234567	dragon	letmein
#9	111111	dragon	iloveyou	111111	trustno1
#10	123123	football	adobe123	baseball	dragon

نصائح للمستخدمين عن للأمن السيبراني

Back up your data

Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.

Keep your operating system up to date

Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.

Install antivirus software

Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.

Choose unique passwords

Create unique passwords for each account – that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.

Set up two-factor authentication (2FA)

Choose to get a code sent to another device like your phone when logging in online – it helps stop hackers getting into your accounts.

Use creative recovery answers

Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.

Be cautious of free WiFi networks

Be careful using free Wifi and hot spots - they are untrusted networks so others could see what you are doing.

Be smart with social media

What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

Don't give out personal info

Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.

Check bank statements regularly

Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.

Get a regular credit check

An annual credit check will alert you if someone else is using your details to get loans or credit.

To report a cyber security problem, visit **www.cert.govt.nz**

التجارة الالكترونية E-COMMERCE

تُعتبر التجارة الإلكترونية واحدة من أبرز التطورات الاقتصادية في العصر الحديث، حيث أدت إلى تغيير جذري في طريقة إجراء الأعمال التجارية. تشمل هذه العملية شراء وبيع المنتجات والخدمات عبر الإنترنت، مما يتيح للمستهلكين الوصول إلى مجموعة واسعة من الخيارات بسهولة ويسر. تتضمن التجارة الإلكترونية مجموعة من الأنشطة مثل التسوق عبر الإنترنت، المزادات الإلكترونية، والخدمات المالية الرقمية. ومع تزايد استخدام الإنترنت وتطور التكنولوجيا، أصبحت التجارة الإلكترونية توفر مزايا كبيرة، مثل توفير الوقت والجهد، وتقليل التكاليف، وزيادة الوصول إلى الأسواق العالمية.

تجذب التجارة الإلكترونية العديد من الشركات، من الصغيرة إلى الكبيرة، حيث يمكنها الوصول إلى جمهور أوسع دون الحاجة إلى استثمارات ضخمة في البنية التحتية. كما أن التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات تلعب دوراً مهماً في تحسين تجربة العميل وزيادة الكفاءة. في ظل هذه التطورات، أصبحت التجارة الإلكترونية جزءاً لا يتجزأ من الاقتصاد العالمي، مما يستدعي فهمًا أفضل لتحدياتها وفرصها في المستقبل.

مفاهيم الخدمات المصرفية الإلكترونية

تُعتبر الخدمات المصرفية الإلكترونية من أبرز مظاهر التطور التكنولوجي في القطاع المالي، حيث توفر مجموعة من الحلول والخدمات عبر الإنترنت.

الخدمات المصرفية عبر الإنترنت

تتميز الخدمات المصرفية عبر الإنترنت بتوفير حلول مالية تتيح للعملاء إجراء معاملاتهم المصرفية بسهولة وأمان من أي مكان وفي أي وقت.

أجهزة الصراف الآلي ATM

هو جهاز إلكتروني يتيح للعملاء القيام بالعديد من المعاملات المالية دون الحاجة إلى زيارة فرع البنك، مثل السحب النقدي، الاستفسار عن الرصيد، تحويل الأموال، دفع الفواتير، وإيداع الأموال (في بعض الحالات).

عادةً ما تكون الأجهزة متاحة على مدار 24 ساعة في مواقع مثل البنوك، المحلات التجارية، والمطارات.

انواع اجهزة الصرف الالي

- **أجهزة مستقلة**
  Standalone ATMs
- توجد في أماكن عامة كالمطارات والفنادق، وغالبًا ما تقدم خدمات أساسية مثل سحب النقود والاستعلام عن الرصيد.

انواع اجهزة الصرف الالي

داخل الفروع (In-Branch ATMs)

توجد داخل الفروع البنكية وتقدم خدمات أوسع مثل الإيداع، تحويل الأموال، وطباعة الكشوفات.

انواع اجهزة الصرف الالي

Deposit ATMs للإيداع

تتيح إيداع النقود أو الشيكات، إضافة إلى المعاملات الأخرى.

انواع اجهزة الصرف الالي

Mobile ATMs متنقلة

توجد في شاحنات تُنقل إلى الفعاليات أو الأحداث

DEBIT CARDS بطاقات الخصم

بطاقة الخصم هي بطاقة إلكترونية مرتبطة مباشرة بحساب العميل الجاري أو التوفير، وتُستخدم للسحب أو الشراء.تُخصم الأموال مباشرة من حساب العميل.

الخدمات الرئيسية لبطاقات الخصم

السحب النقديالشراء من المتاجر ((POSالشراء عبر الإنترنت الدفع التلقائي للفواتير إدارة النفقات

فوائد بطاقات الخصم

1. لا حاجة لحمل النقود،
2. مقبولة في نطاق واسع.
3. تساعد في التحكم المالي وتجنب الديون.
4. الأمان باستخدام PIN وتقنيات تحقق إلكترونية.

التكامل والامان

التكامل بين أجهزة الصراف الآلي وبطاقات الخصمالبطاقة أداة رئيسية للوصول إلى خدمات **ATM.**توفرراحة وأمانًا عاليين.تتيح إدارة الحسابات بسهولة.

الاعتبارات الأمنية

الحفاظ على سرية رقم **PIN.**استخدام الأجهزة في أماكن آمنة وغيرمعزولة.مر اقبة الحساب بانتظام وخاصة عند التسوق عبر الإنترنت.

مفاهيم مكملة في الخدمات المصرفية الإلكترونية

الخدمات المصرفية عبر الهاتف:

تتيح للعميل التواصل مع البنك هاتفيًا لتنفيذ خدمات مثل الاستعلام عن الرصيد، تحويل الأموال، أو إيقاف البطاقة.

الخدمات المصرفية عبر الرسائل النصية:

استلام رسائل قصيرة تحتوي على معلومات مثل الرصيد الحالي أو إشعار بحدوث معاملة مالية.

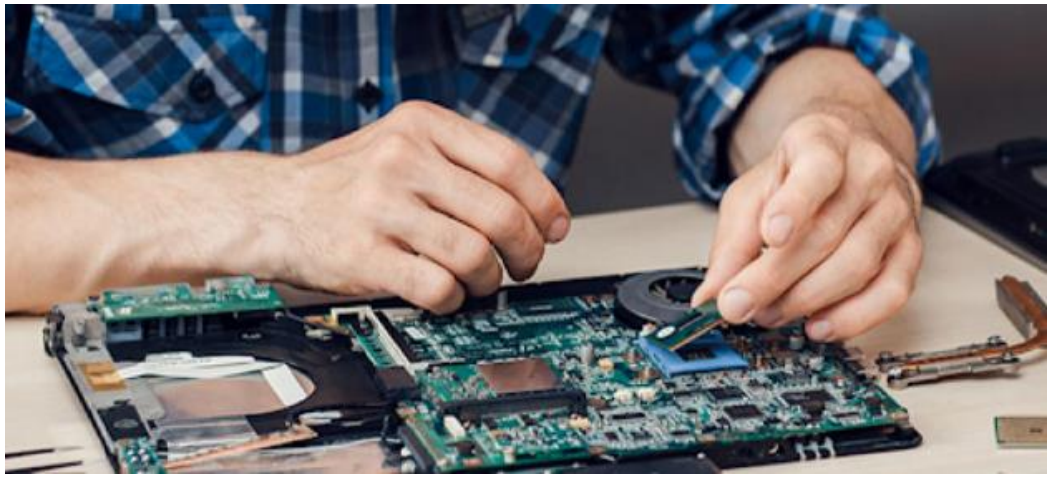
التنبيهات الإلكترونية:

إشعارات فورية عبر الرسائل النصية أو البريد الإلكتروني تُرسل تلقائيًا عند حدوث أي حركة على الحساب.

الخدمات المصرفية عبر الهاتف المحمول:

تطبيقات ذكية تمكن العميل من إدارة حساباته بسهولة، مثل تحويل الأموال، دفع الفواتير، أو الاطلاع على كشف الحساب

استكشاف أخطاء الكمبيوتر وإصلاحها

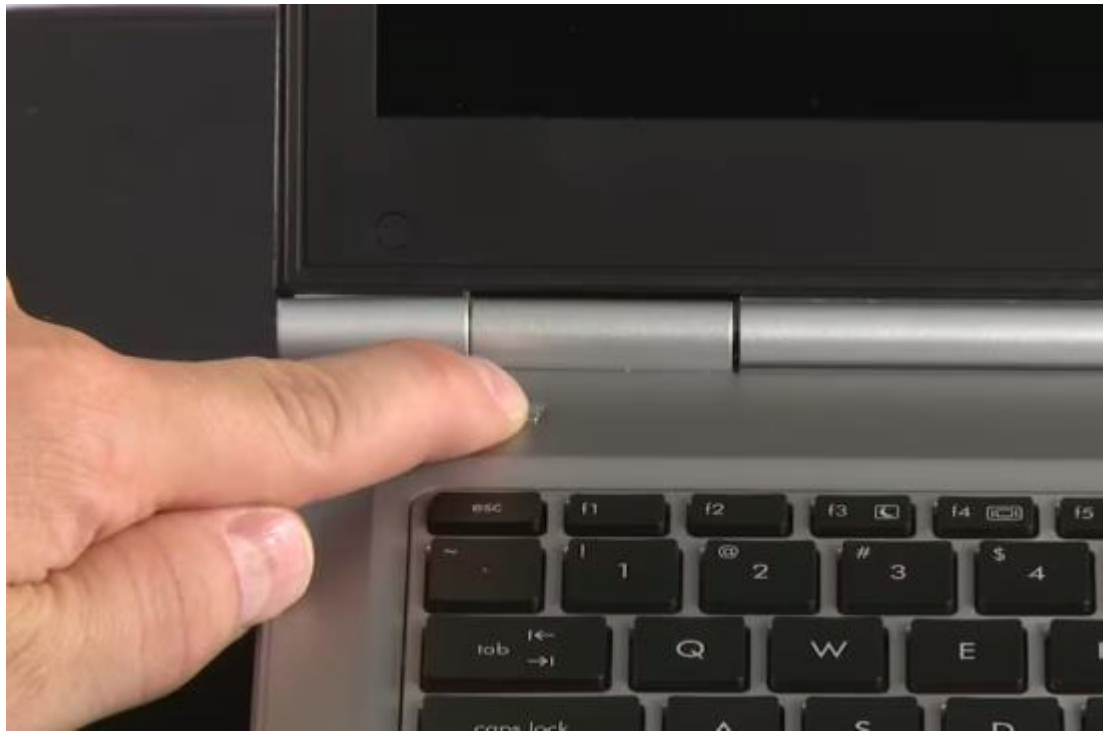


عد عملية استكشاف الأخطاء وإصلاحها في أجهزة الكمبيوتر من الجوانب الأساسية للتعامل مع التكنولوجيا الحديثة .مع الاعتماد المتزايد على أجهزة الكمبيوتر في العمل والتعليم والترفيه، تصبح مواجهة الأخطاء التقنية أمرًا شائعًا، مما يستدعي وجود مهارات لمعالجتها بسرعة وفعالية.

- تشمل الأخطاء الشائعة في أجهزة الكمبيوتر:
  - أعطال النظام
  - مشاكل الأداء
  - تعطل البرامج
  - فقدان البيانات
  - أعطال الأجهزة)ناتجة عن أسباب داخلية مثل البرامج الضارة أو تلف النظام، أو أسباب خارجية مثل انقطاع الكهرباء(

- تتطلب عملية الاستكشاف خطوات منهجية لفهم سبب المشكلة وتحديد الحلول المناسبة .تبدأ العملية بتحديد الأعراض، فهم المشكلة، تحليل الأسباب المحتملة، ثم تطبيق الحلول الممكنة .يمكن أن تتراوح الحلول من إعادة تشغيل الجهاز إلى إصلاحات متقدمة تتطلب معرفة تقنية متخصصة.

مشاكل الاجهزة



1.الجهاز لا يعمل:(Dead Computer)

- **الأعراض :**عدم استجابة الجهاز عند التشغيل أو عدم ظهور مؤشرات طاقة.
- **الحلول:**
  - تأكد من توصيل الجهاز بمصدر طاقة صحيح.
  - تحقق من كابل الطاقة ومنفذ الكهرباء.
  - افحص وحدة تزويد الطاقة.(PSU)

مشاكل الاجهزة

ارتفاع درجة حرارة الجهاز:

- **الأعراض :**إيقاف تشغيل مفاجئ، تباطؤ الأداء، سماع أصوات مروحة عالية.
- **الحلول:**
  - نظف فتحات التهوية والمراوح.
  - تأكد من وضع الجهاز في مكان جيد التهوية.
  - استبدل معجون التبريد إذا لزم الأمر.

مشاكل الاجهزة

3.تعطل الشاشة:(Display Issues)

- **الأعراض :**شاشة سوداء، وميض، صورة غير واضحة.
- **الحلول:**
  - تأكد من توصيل الكابلات بشكل صحيح.
  - جرب تغيير الشاشة أو كابل التوصيل.
  - افحص إعدادات كرت الشاشة أو استبدله إذا لزم.

4.مشاكل في التخزين:(Hard Drive/SSD Issues)

- **الأعراض :**بطء الجهاز، عدم القدرة على حفظ الملفات، أصوات غير طبيعية.
- **الحلول:**
  - فحص القرص باستخدام أدوات مثل .CHKDSK
  - استبدال القرص في حال تلفه واستخدام برامج استرداد البيانات.

مشاكل الاجهزة

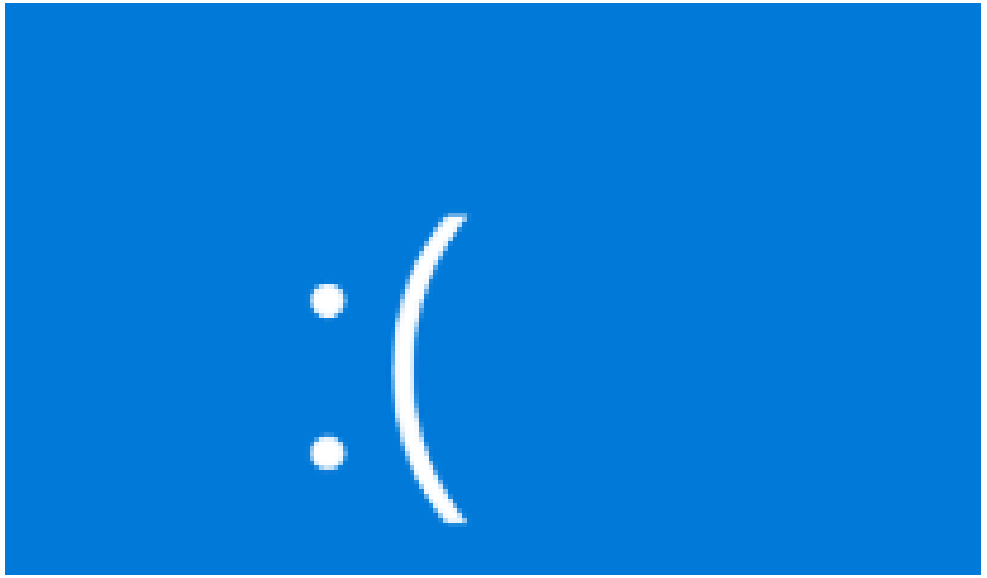
3.تعطل الشاشة:(Display Issues)

- **الأعراض :**شاشة سوداء، وميض، صورة غير واضحة.
- **الحلول:**
  - تأكد من توصيل الكابلات بشكل صحيح.
  - جرب تغيير الشاشة أو كابل التوصيل.
  - افحص إعدادات كرت الشاشة أو استبدله إذا لزم.

4.مشاكل في التخزين:(Hard Drive/SSD Issues)

- **الأعراض :**بطء الجهاز، عدم القدرة على حفظ الملفات، أصوات غير طبيعية.
- **الحلول:**
  - فحص القرص باستخدام أدوات مثل .CHKDSK
  - استبدال القرص في حال تلفه واستخدام برامج استرداد البيانات.

"الشاشة الزرقاء" في WINDOWS



يمكن أن تحدث أخطاء الشاشة الزرقاء (تسمى أيضا *عمليات التحقق من الأخطاء* أو *أخطاء رمز STOP* أو *أخطاء النواة* أو *أخطاء BSOD*) إذا كانت هناك مشكلة خطيرة تتسبب في إيقاف تشغيل Windows أو إعادة تشغيله بشكل غير متوقع لحماية نفسه من فقدان البيانات. قد ترى رسالة تقول: "تم إيقاف تشغيل Windows لمنع حدوث تلف بالكمبيوتر" أو رسالة مماثلة.

خطوات استكشاف الأخطاء الأساسية وإصلاحها لأخطاء الشاشة الزرقاء

افصل الأجهزة الجديدة:

إذا أضفت أجهزة قبل ظهور الخطأ، افصلها وأعد تشغيل الكمبيوتر.

ابدأ في الوضع الآمن:

إذا لم يتمكن الكمبيوتر من الإقلاع، شغله في الوضع الآمن وجرب الإصلاحات من هناك.

افحص إدارة الأجهزة:

افتح "إدارة الأجهزة".

إذا وجدت علامة (!) على جهاز، حدّث تعريفه أو عطّله أو احذفه.

تحقق من مساحة التخزين:

تأكد أن لديك 10-15٪ مساحة حرة على القرص الصلب.

حدث **Windows:**

اذهب إلى الإعدادات > **Windows Update** وتحقق من وجود تحديثات.

استخدم استعادة النظام:

إذا لم تنجح الحلول، استعد النظام إلى نقطة سابقة.

ثانيًا: مشاكل البرامج(SOFTWARE ISSUES)

1.تجمد النظام:(System Freezes)

- **الأعراض :**عدم استجابة الجهاز عند تشغيل التطبيقات.
- **الحلول:**
  - أعد تشغيل الجهاز.
  - تحقق من تحديثات نظام التشغيل أو التعريفات.
  - تأكد من توفر موارد كافية (RAM و.CPU)

2.الأخطاء البرمجية:(Software Errors)

- **الأعراض :**ظهور رسائل خطأ عند تشغيل البرامج.
- **الحلول:**
  - أعد تثبيت البرنامج.
  - تحقق من توافق البرنامج مع النظام.
  - قم بتثبيت التحديثات.

ثانيًا: مشاكل البرامج(SOFTWARE ISSUES)

3.الفيروسات والبرمجيات الضارة:

- **الأعراض :**تباطؤ الجهاز، ظهور إعلانات، حذف ملفات.
- **الحلول:**
  - فحص الجهاز ببرنامج مكافحة الفيروسات.
  - إزالة البرامج المشبوهة.
  - تحديث برنامج مكافحة الفيروسات بانتظام.

4.بطء الأداء:(Slow Performance)

- **الأعراض :**بطء في فتح الملفات أو تشغيل التطبيقات.
- **الحلول:**
  - إغلاق البرامج غير الضرورية.
  - إلغاء تثبيت البرامج غير المستخدمة.
  - تنظيف الملفات المؤقتة باستخدام."Disk Cleanup"

ثانيًا: مشاكل البرامج(SOFTWARE ISSUES)

5.مشاكل الشبكة والإنترنت:

- **الأعراض :**عدم الاتصال بالإنترنت أو بطء التصفح.
- **الحلول:**
  - تحقق من اتصال الكابلات أو إعدادات الواي فاي.
  - أعد تشغيل جهاز التوجيه.(Router)
  - استخدم أمر "ipconfig /renew" لإصلاح إعدادات الشبكة.

نصائح مهمة

. تحديث نظام التشغيل والتعريفات بانتظام.

. استخدام برامج مكافحة الفيروسات الموثوقة.

. عمل نسخ احتياطية منتظمة للبيانات.

. تنظيف مكونات الجهاز دوريًا.

- تثبيت البرامج من مصادر موثوقة فقط

تقنيات وأدوات استكشاف الأخطاء الأساسية

تُعد تقنيات استكشاف الأخطاء من المهارات الأساسية لضمان استمرارية العمل. تعتمد على اتباع نهج منهجي لتحديد السبب الجذري للمشكلة والعمل على حلها باستخدام أدوات مثل:

- مدير المهام(Task Manager)
- أدوات الشبكة) مثل ping و(tracert
- برامج فحص النظام

الأهداف:

- تحسين أداء الأنظمة
- ضمان أمان البيانات
- تقليل تكاليف الصيانة

خطوات مهمة

1.الفهم الأولي للمشكلة:

- استفسر عن طبيعة المشكلة ومتى بدأت وأين.
- تحقق من التغييرات الأخيرة مثل تحديثات البرامج أو تثبيت الأجهزة.

2.التحقق من الاتصالات الأساسية:

- تأكد من توصيل جميع الكابلات بشكل صحيح.
- افحص الأجهزة الملحقة (ماوس، لوحة مفاتيح، شاشة).

3.تحديد المشكلة:

- فصل الأجهزة والبرامج لتحديد مصدر المشكلة.
- تصنيف المشكلة إلى عطل مادي (Hardware) أو برمجي (Software) أو شبكي.(Network)

4.اتباع نهج منهجي:

- استخدام طريقة الاستبعاد، بحذف أو تعطيل العناصر المشبوهة خطوة بخطوة.

افضل الممارسات

. فحص الجهاز دوريًا.
. أخذ نسخ احتياطية منتظمة.
. توثيق خطوات الاستكشاف لضمان عدم تكرار المشاكل.

الذكاء الاصطناعي

الذكاء الاصطناعي (Artificial Intelligence) هو فرع من فروع علوم الحاسوب يُعنى بتصميم وتطوير أنظمة وبرمجيات قادرة على أداء مهام تتطلب عادةً ذكاءً بشريًا، مثل التعلم، والاستدلال، واتخاذ القرار، وحل المشكلات. ويهدف الذكاء الاصطناعي إلى تمكين الآلات من محاكاة العمليات الإدراكية البشرية، بما في ذلك الفهم، والتخطيط، والتفاعل مع البيئة بطريقة ذكية وفعالة.

الذكاء الاصطناعي

الذكاء الاصطناعي (Artificial Intelligence) هو فرع من فروع علوم الحاسوب يُعنى بتصميم وتطوير أنظمة وبرمجيات قادرة على أداء مهام تتطلب عادةً ذكاءً بشريًا، مثل التعلم، والاستدلال، واتخاذ القرار، وحل المشكلات. ويهدف الذكاء الاصطناعي إلى تمكين الآلات من محاكاة العمليات الإدراكية البشرية، بما في ذلك الفهم، والتخطيط، والتفاعل مع البيئة بطريقة ذكية وفعالة.

نظرة عامة عن الذكاء الاصطناعي (ARTIFICIAL INTELLIGENCE)

- الذكاء الاصطناعي هو مجال من علوم الحاسب الآلي يركز على تطوير أنظمة وتطبيقات قادرة على القيام بمهام تتطلب عادةً ذكاء بشري والذي يشمل القدرات المعرفية مثل التعلم والتفكير والاستنتاج والتخطيط وحل المشكلات واتخاذ القرارات.

- الهدف الرئيسي للذكاء الاصطناعي هو محاكاة وتحسين القدرات العقلية البشرية باستخدام التكنولوجيا الحاسوبية المتقدمة.

تاريخ الذكاء الاصطناعي

1. **المرحلة الأولى (1950s):**
    1. **1950:** نشر آلان تورينج ورقة بعنوان "الآلات الحاسوبية والذكاء" التي قدم فيها "اختبار تورينج" لقياس قدرة الآلة على التفكير.
    2. 1956: عقد أول مؤتمر للذكاء الاصطناعي في دارتموث، حيث تم صياغة مصطلح "الذكاء الاصطناعي".
2. **المرحلة الثانية (1960s-1970s):**
    1. **1961:** أول روبوت صناعي (Unimate) يستخدم في خط إنتاج جنرال موتورز.
    2. 1966: تطوير نظام ELIZA، أول برنامج معالجة لغة طبيعية يمكنه محاكاة محادثة مع الإنسان.
    3. 1969: تطوير نظام Shakey، أول روبوت يمكنه اتخاذ قرارات بناءً على بيئته.
3. **المرحلة الثالثة (1980s-1990s):**
    1. **1980:** استخدام الأنظمة الخبيرة في الصناعة، مثل نظام XCON لشركة ديجيتال إيكويبمنت كوربوريشن.
    2. 1987: تراجع في التمويل والاهتمام بالذكاء الاصطناعي بسبب الصعوبات التقنية والاقتصادية (يطلق عليه "شتاء الذكاء الاصطناعي").
    3. 1997: هزيمة جاري كاسباروف، بطل العالم في الشطرنج، أمام الكمبيوتر العملاق IBM Deep Blue.
    4. **2020s:** استخدام الذكاء الاصطناعي في العديد من المجالات مثل الرعاية الصحية، التعليم، والأتمتة الصناعية، وزيادة الأبحاث في الذكاء الاصطناعي

تاريخ الذكاء الاصطناعي

1. المرحلة الرابعة (2000s):
    1. **2000**: تطبيقات الذكاء الاصطناعي في الحياة اليومية، مثل أنظمة التوصية ومحركات البحث.
    2. **2005**: تطوير أول سيارة ذاتية القيادة قادرة على إكمال سباق DARPA Grand Challenge.
    3. **2009**: تطوير نظام IBM Watson الذي هزم أبطال لعبة Jeopardy! في عام 2011.
2. المرحلة الخامسة (2010s-2020s):
    1. **2012**: نجاح كبير في التعلم العميق مع فوز نموذج AlexNet في مسابقة ImageNet.
    2. **2016**: فوز AlphaGo، نظام الذكاء الاصطناعي من Google DeepMind، على بطل العالم في لعبة Go.

لماذا يهتم الباحثون بالذكاء الاصطناعي؟ لماذا تتوجه الشركات والمؤسسات نحو تطبيقات الذكاء الاصطناعي بشكل متزايد ؟

أهداف الذكاء الاصطناعي

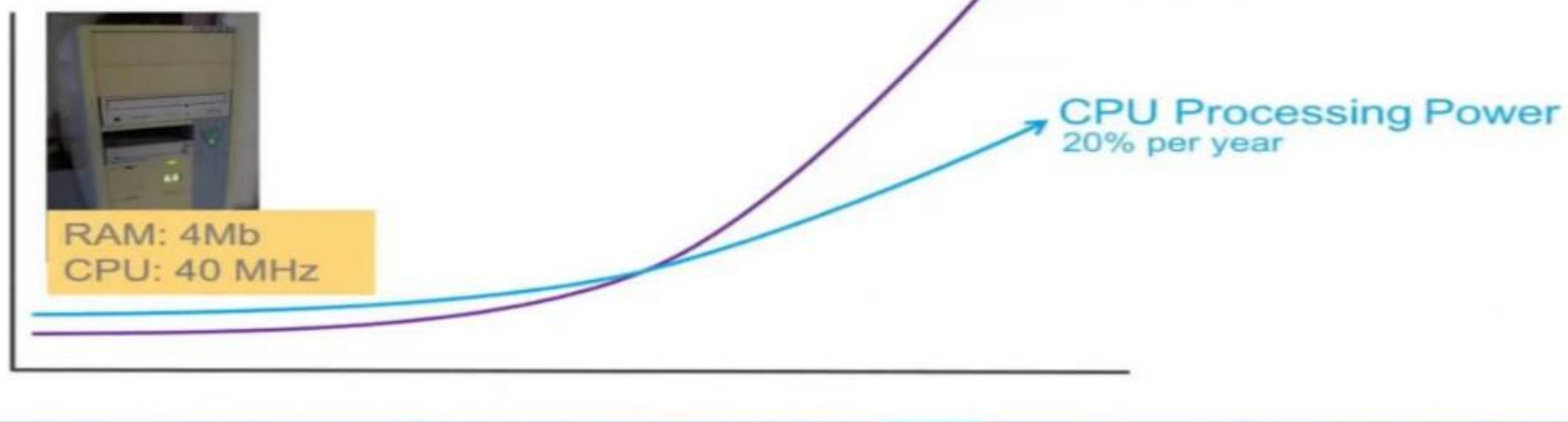
- محاكاة وتقليد القدرات المعرفية البشرية، مثل القدرة على التعلم والاستنتاج والتفكير المنطقي.
- تطوير تطبيقات قادرة على أداء مهام معقدة بكفاءة وموثوقية أكبر من البشر.
- تخطي قدرات الإنسان من خلال تطوير أنظمة ذكاء اصطناعي فائقة التطور وواسعة النطاق.
- المساعدة في حل المشكلات العالمية الصعبة في مجالات مثل الطب والهندسة والإدارة

خصائص وميزات تطبيقات الذكاء الاصطناعي

- الأتمتة او التشغيل الآلي (Automation)
- الموثوقية والدقة (Reliability and Accuracy)
- الإتاحة (Availability)
- الكفاءة (Efficiency) والانتاجية
- تحليل البيانات الكبيرة
- القدرة على التعلم والتكيف والتحسين
- تخفيف المخاطر (Risk mitigation)

ممكنات تطور الذكاء الاصطناعي

- Big Data
- Processing power



أنواع الذكاء الاصطناعي

الذكاء الاصطناعي الفائق (ASI)

الذكاء الاصطناعي الفائق يتجاوز قدرات الذكاء البشري في جميع المجالات .هذا النوع من الذكاء الاصطناعي هو هدف طموح للباحثين، لكن تحقيقه يُعتبر كبيرًا وقد يكون له آثار هائلة على المجتمع.

الذكاء الاصطناعي العام (AGI)

الذكاء الاصطناعي العام يشير إلى نظام ذكاء اصطناعي قادر على التفكير والتعلم والتخطيط وحل المشكلات بنفس التي يفعلها البشر .هذا النوع من الذكاء الاصطناعي لا يزال في مراحل البحث والتطوير.

الذكاء الاصطناعي الضيق (ANI)

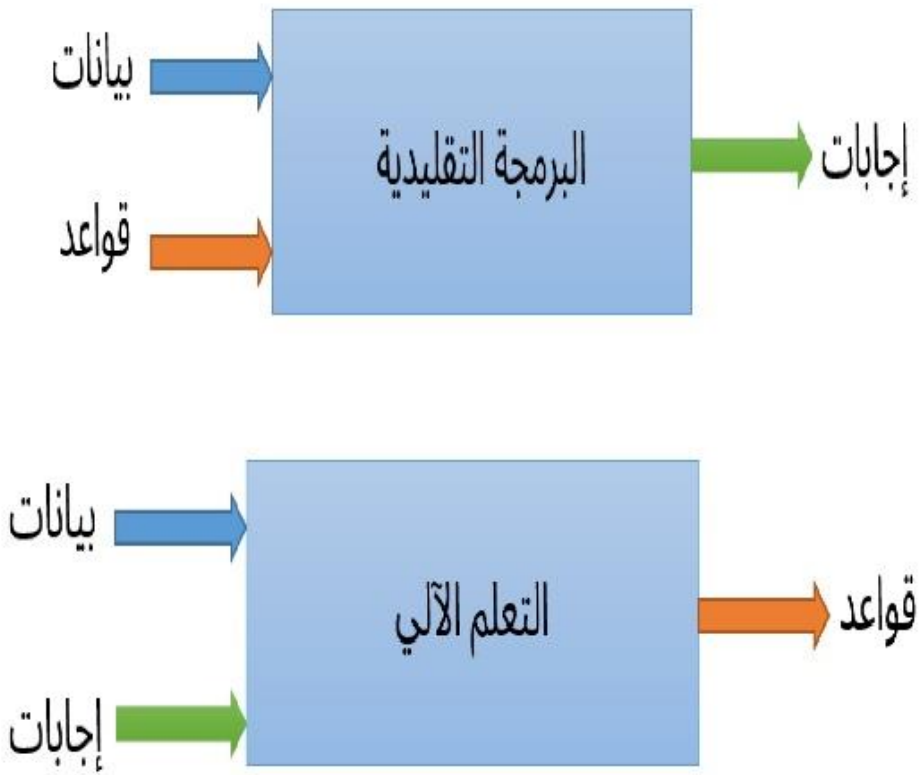
يتميز الذكاء الاصطناعي الضيق بقدرته على القيام بمهام محددة وموجهة بشكل جيد، مثل لعب الشطرنج أو التعرف على الوجوه .هذا النوع من الذكاء الاصطناعي لا يتمتع بالقدرة على التعميم أو حل مشكلات جديدة خارج نطاق تدريبه.

البرمجة التقليدية والذكاء الاصطناعي

نشأ علم التعلم الآلي عندما بدأ علماء الحاسوب بطرح الأسئلة التالية:

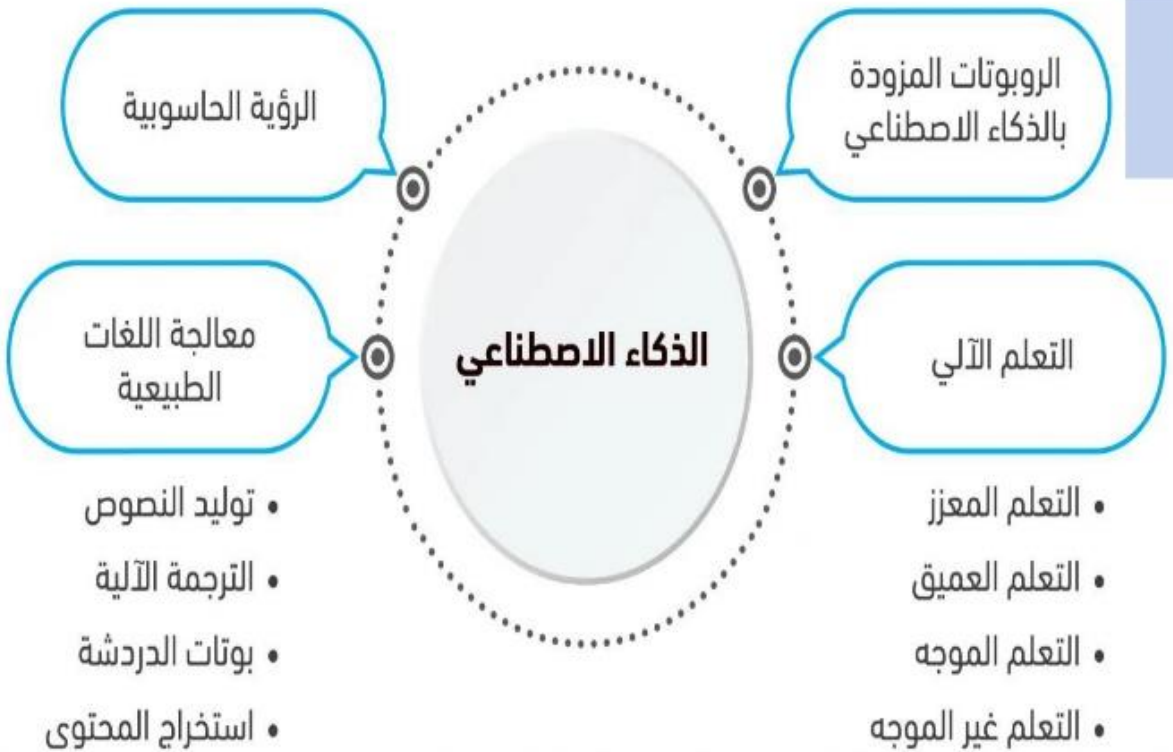
- **نحن البشر نتعلم من التجارب السابقة أما الآلات فهي تفعل ما نمليه عليها فقط فهل يمكن أن نتمكن من تدريب هذه الآلات كي تتعلم من البيانات والخبرات السابقة وتحاكي طريقة تفكيرنا وتتمكن من التعلم والفهم والاستنتاج دون تدخلنا؟**
- **هل يمكن للحواسيب أن تفعل ما نفعله وبالطريقة التي نريدها، وأن تتعلم من تلقاء نفسه كيفية أداء مهمة محددة؟**
- **هل يمكن للحواسيب والآلات أن تفاجئنا وتتعلم من خلال البيانات من تلقاء نفسه بدلًا من قيام المبرمجين بصياغة قواعد معالجة البيانات لها بشكل يدوي؟**

كل هذه التساؤلات فتحت الباب أمام نموذج برمجة بديل عن أسلوب البرمجة الكلاسيكية التي يُدخل فيها البشر القواعد ضمن برامج حاسوبية ويحددون بدقة البيانات التي يجب معالجتها وفقًا لهذه القواعد ويكون المخرجات إجابات محددة ناتجة عن عمليات المعالجة.

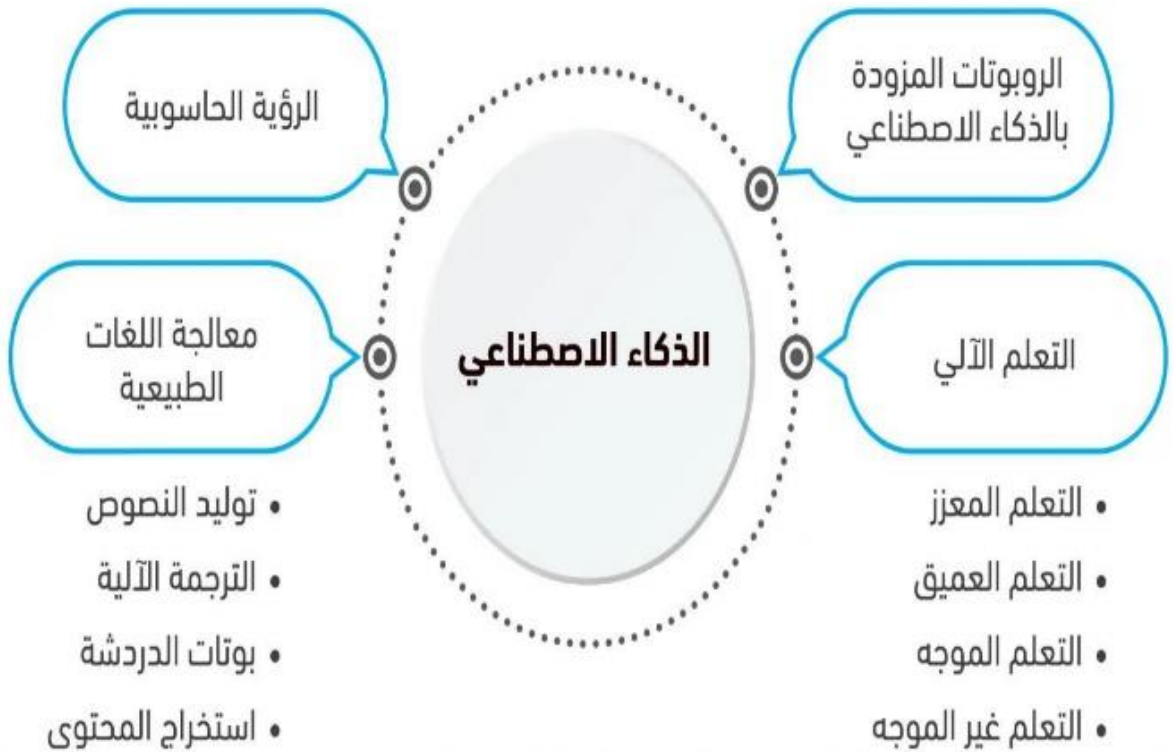


أهم فروع الذكاء الاصطناعي

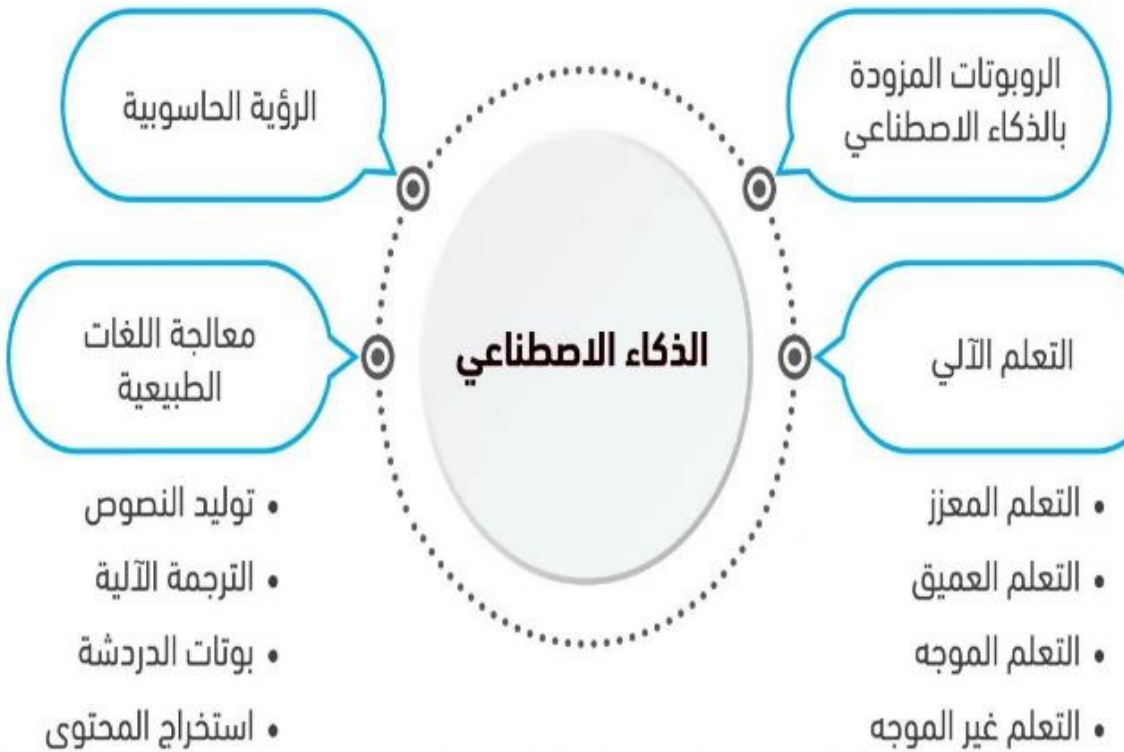
الروبوتات هي آلات ذكية قادرة على تنفيذ مهام محددة بشكل مستقل، وتُستخدم في مجالات متنوعة مثل التصنيع والخدمات.



أهم فروع الذكاء الاصطناعي



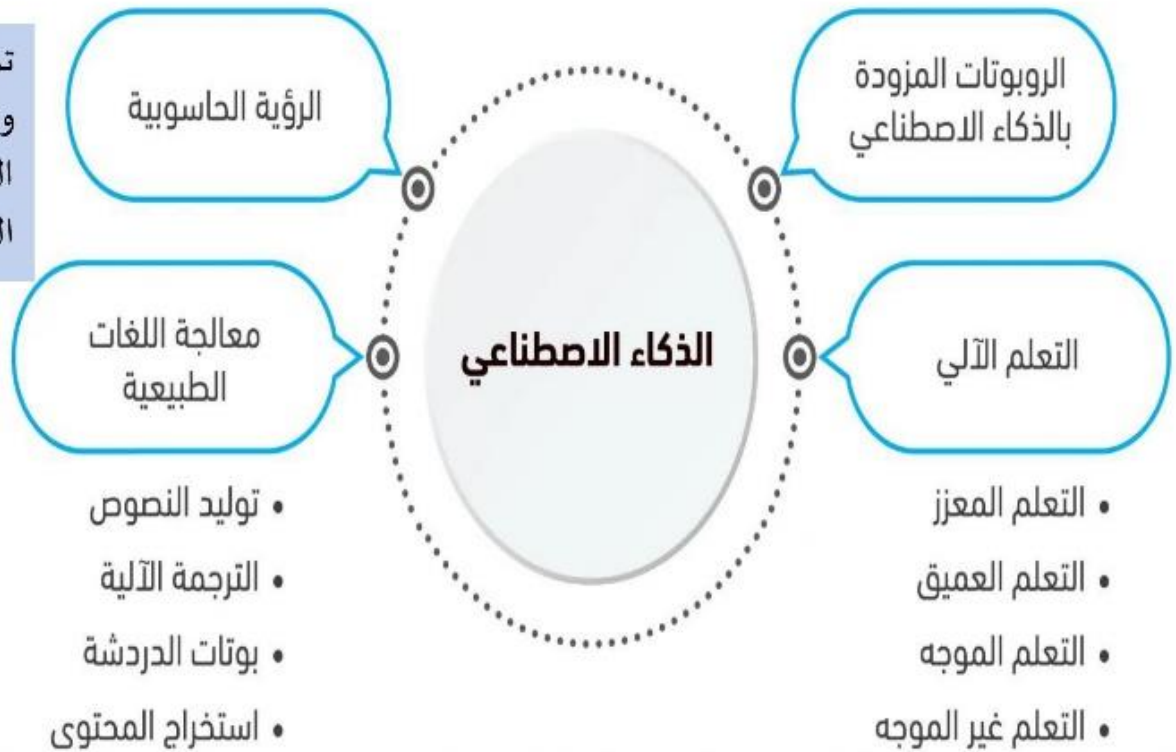
أهم فروع الذكاء الاصطناعي



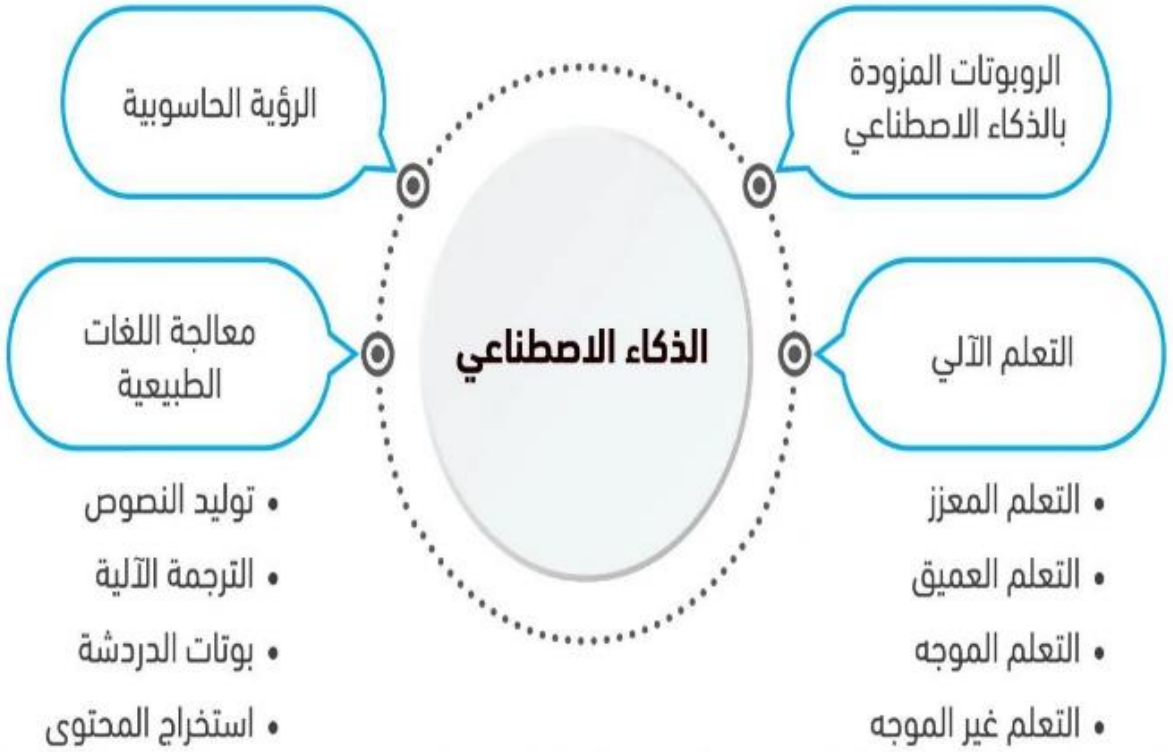
يُعتبر تعلم الآلة أساس الذكاء الاصطناعي، حيث يُمكّن النظم من التعلم والتحسين من تجاربها الحاجة إلى برمجة صريحة.

أهم فروع الذكاء الاصطناعي

تمكن الآلات من تفسير وفهم الصور والفيديوهات. تشمل التطبيقات التعرف على الوجوه، والتعرف على الأشياء، والتحليل الطبي للصور.



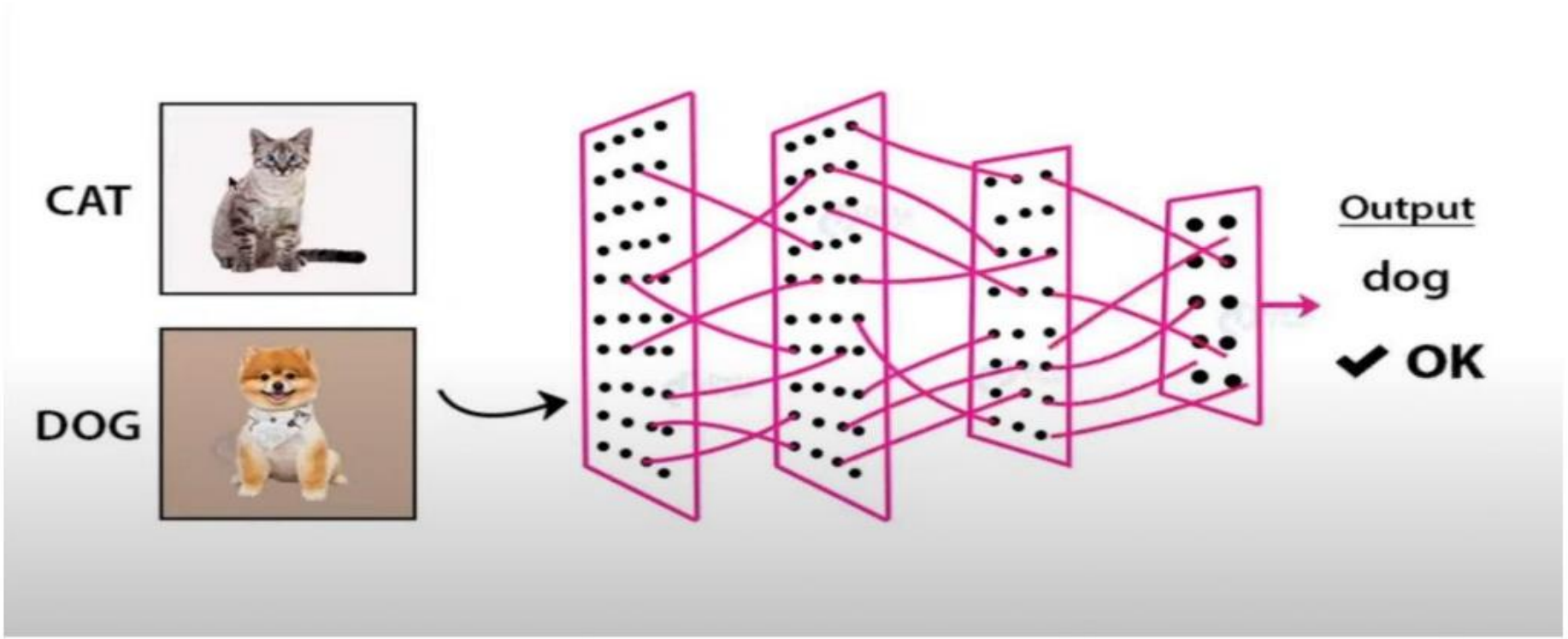
أهم فروع الذكاء الاصطناعي



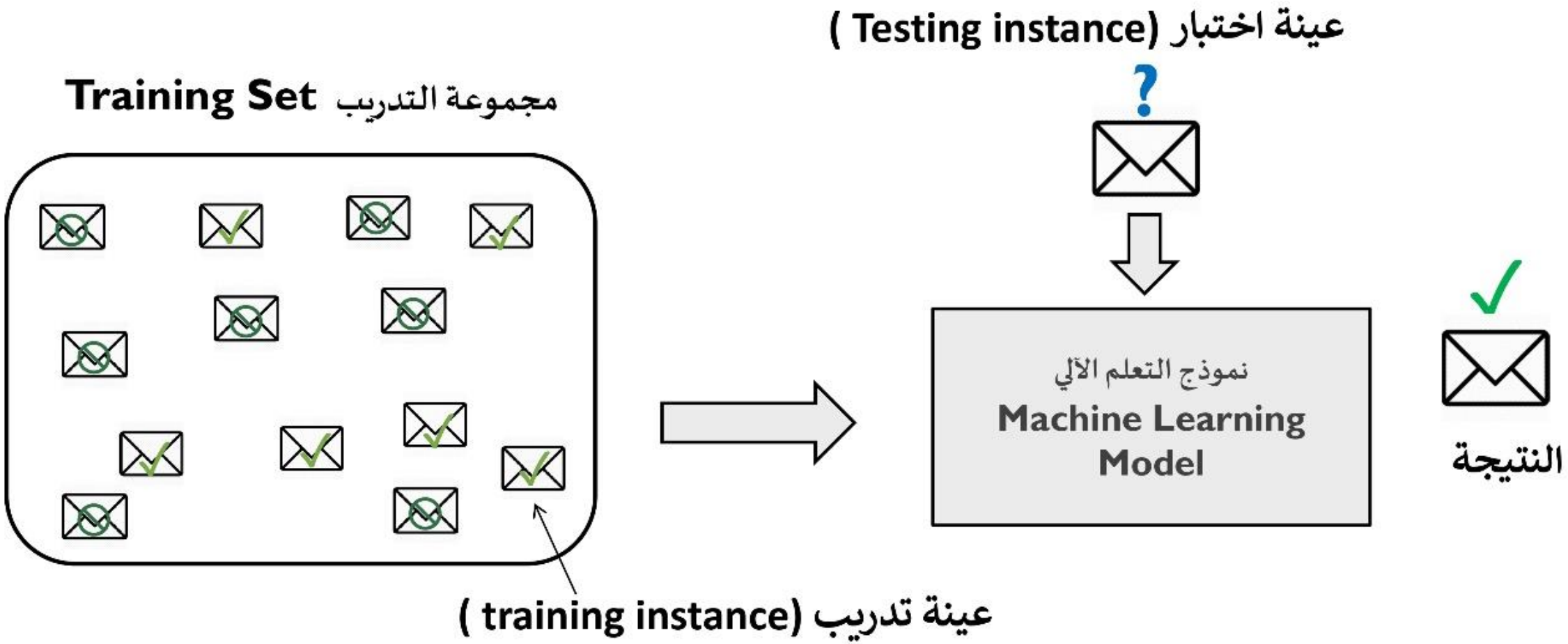
معالجة اللغة الطبيعية تُمكّن من فهم اللغة البشرية وتحليلها مما يوفر تفاعلات طبيعية بين البشر والآلات.


Text
Sound
Photo
Video
Logs
Data
بيانات
Model
نماذج
Machine Learning
Deep Learning
Transfer Learning

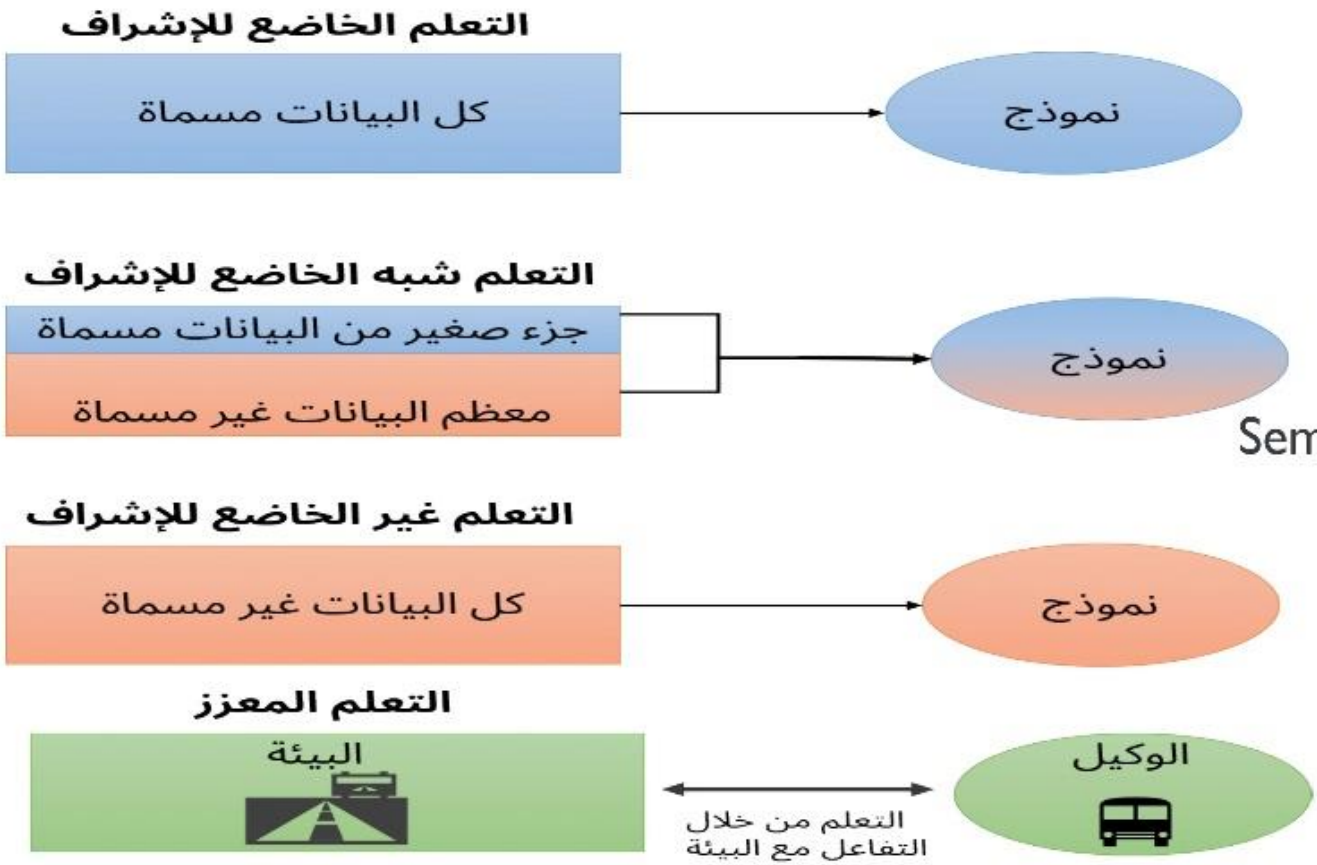
MACHINE LEARNING تعلم الآلة



مثال : تصفية البريد العشوائي (SPAM FILTERING)

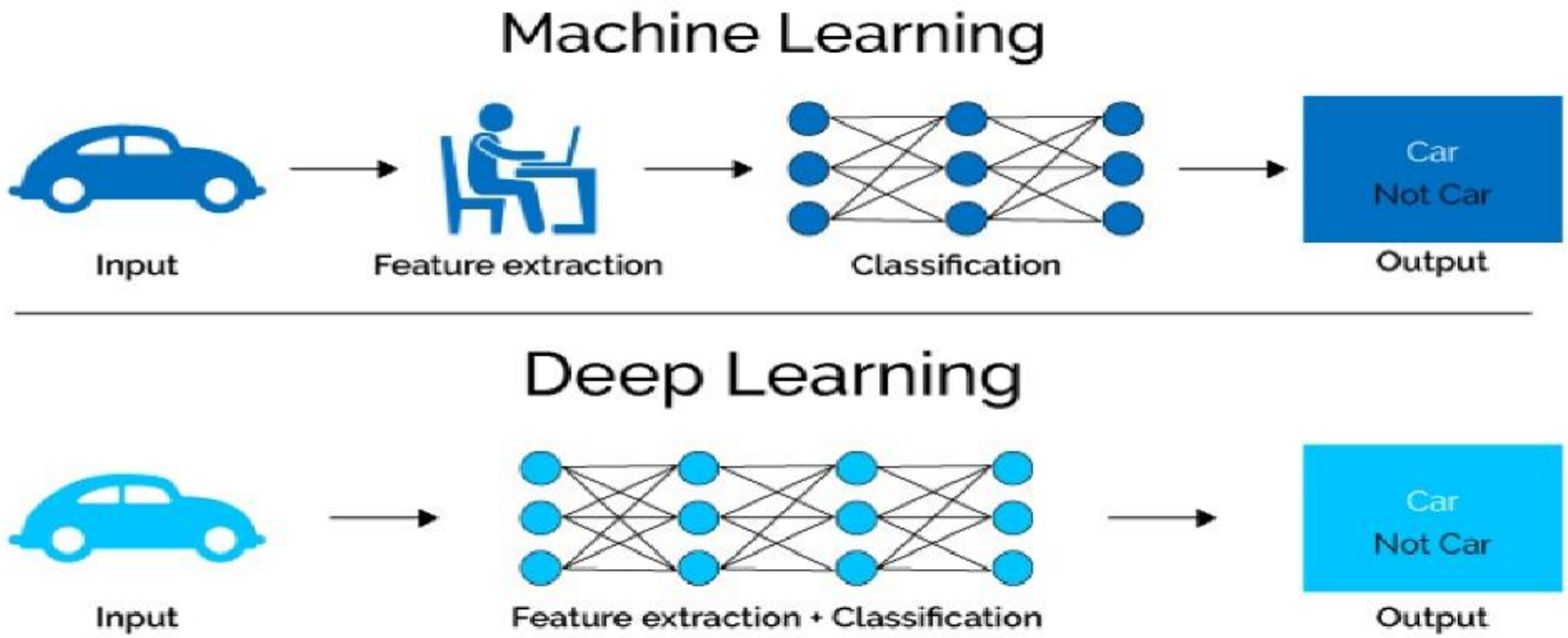


أنواع تعلم الآلة

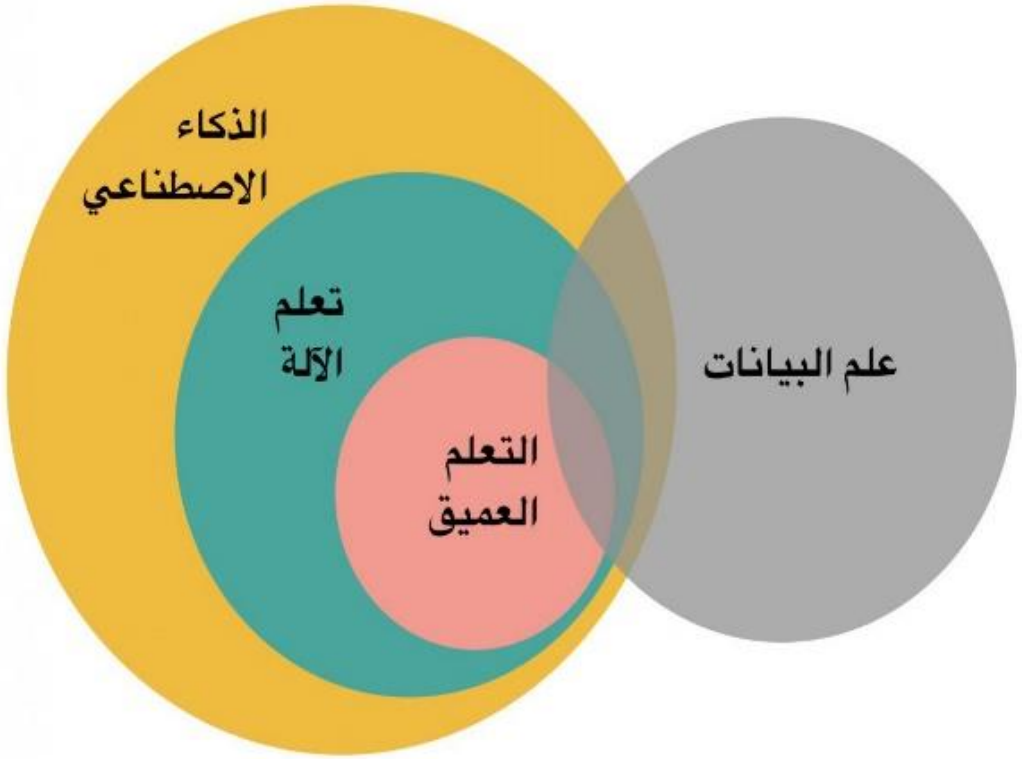


1. التعلم الخاضع للإشراف Supervised learning
2. التعلم غير الخاضع للإشراف UnSupervised learning
3. التعلم شبه الخاضع للإشراف Semi-Supervised Learning
4. التعلم المُعزز Reinforcement Learning

الفرق بين تعلم الالة والتعلم العميق



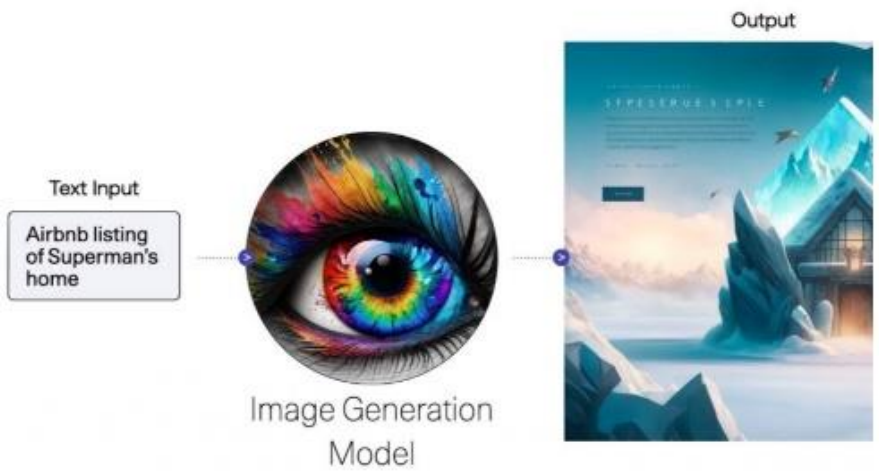
التعلم العميق

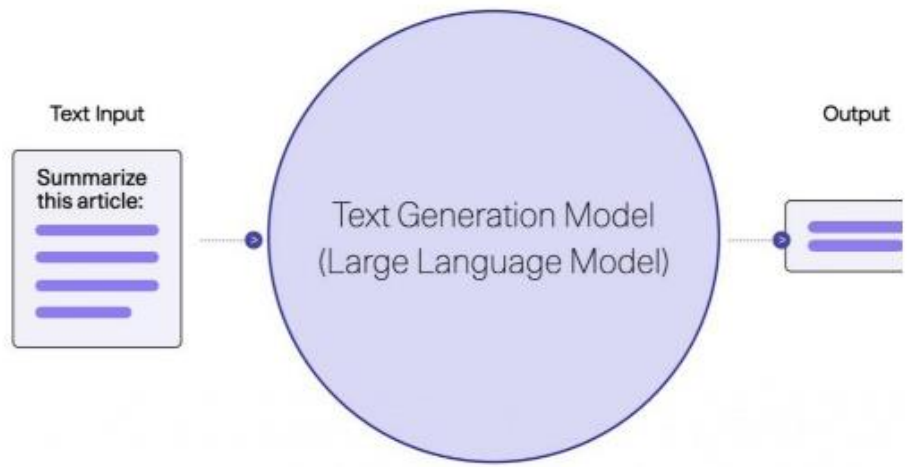


- التعلم العميق هو مجموعة فرعية من تعلم الآلة، يركز على استخدام الشبكات العصبية العميقة لتحليل البيانات والتعلم منها
- وهو يستخدم الشبكات العصبية الاصطناعية التي تتكون من **طبقات متعددة (عميقة)** لمعالجة البيانات. يتميز التعلم العميق بقدرته على معالجة كميات كبيرة من البيانات والتعلم من البيانات غير المهيكلة مثل الصور والنصوص والصوت. من أشهر نماذج التعلم العميق هي الشبكات العصبية التلافيفية (CNN)والشبكات العصبية التكرارية (RNN).

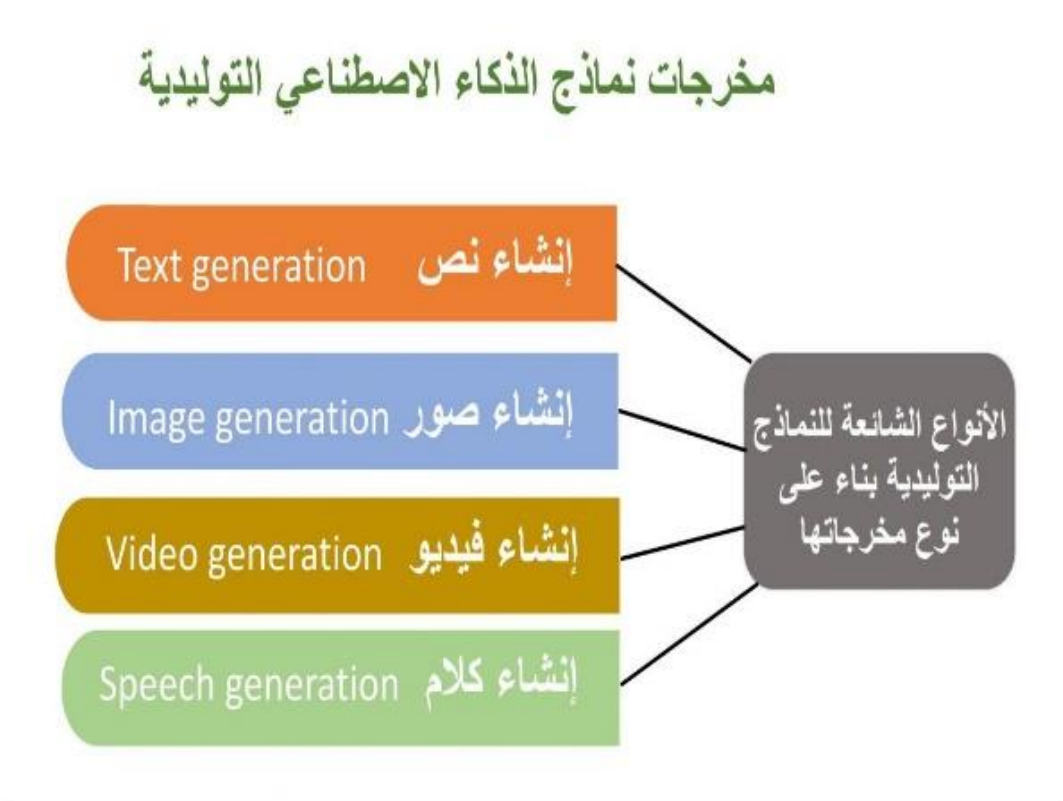
الذكاء التوليدي

- يشمل تطوير خوارزميات يمكنها توليد محتوى جديد مثل النصوص، والصور، والموسيقى.
- تبنى على نماذج التعلم العميق





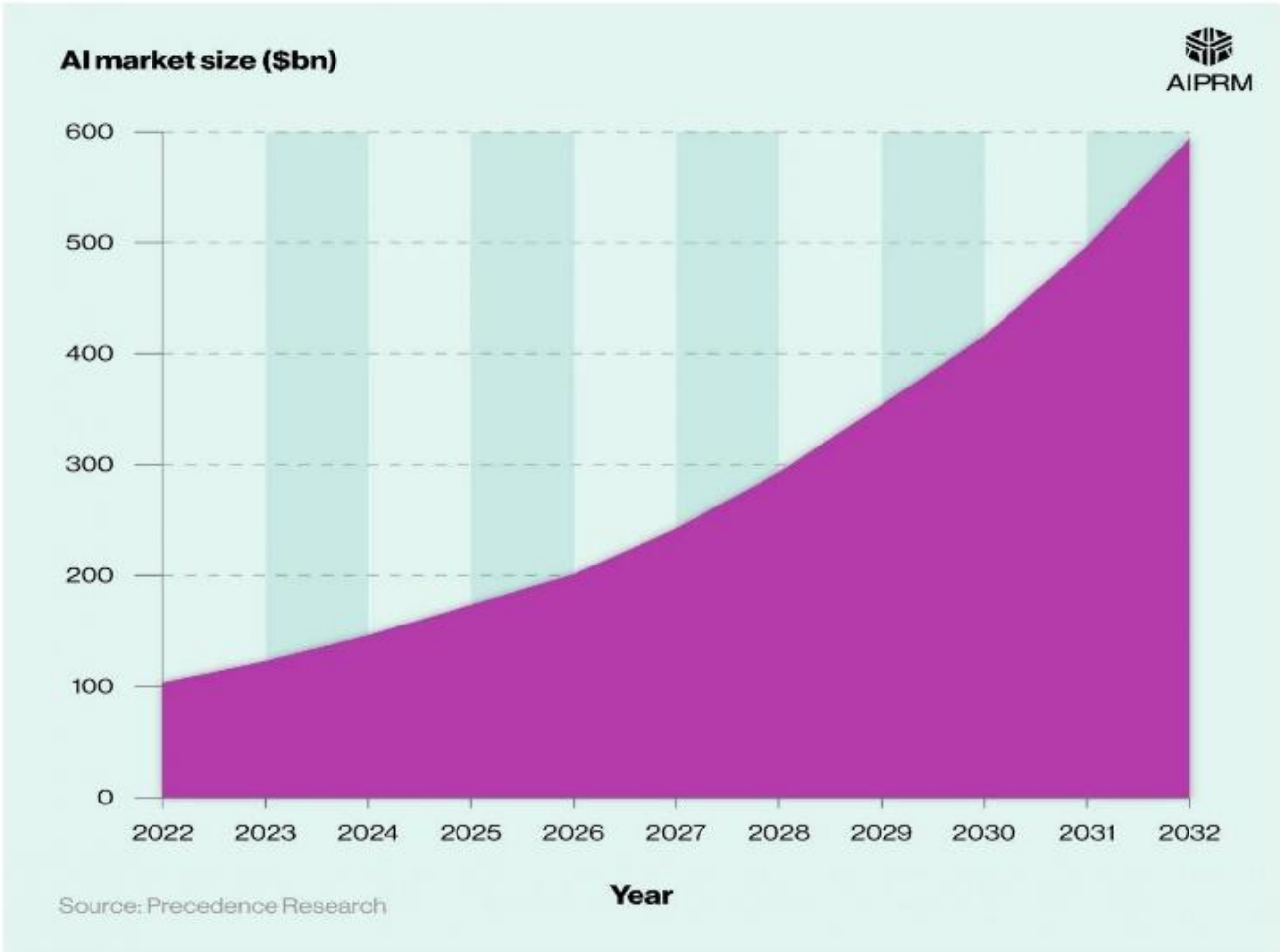
الذكاء التوليدي



د. هند الخليفة (2923). مقدمة في الذكاء الاصطناعي التوليدي

أشهر نماذج مبنيه على الذكاء التوليدي

إحصائيات نمو سوق الذكاء الاصطناعي

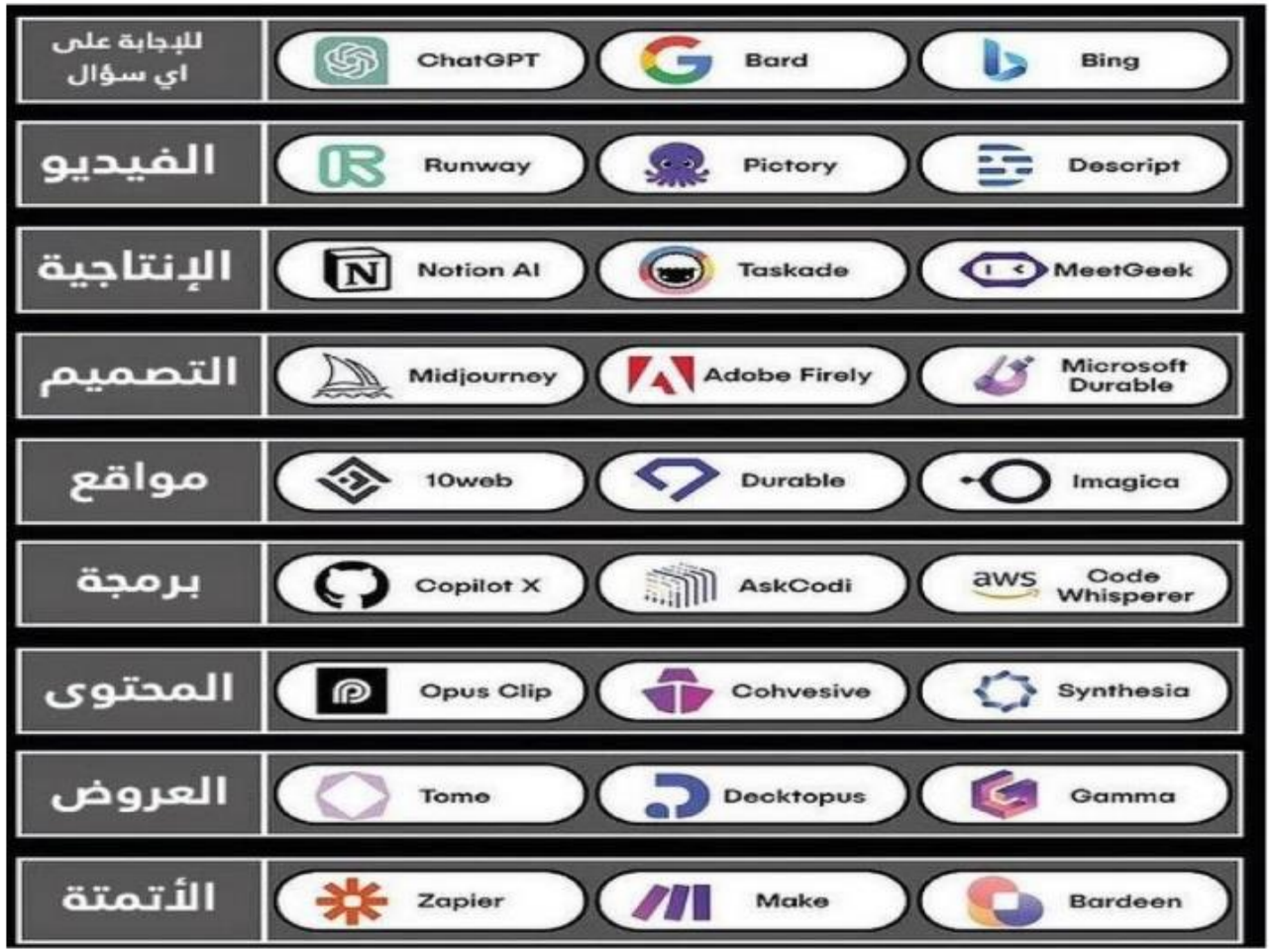


- تُظهر إحصائيات نمو الذكاء الاصطناعي أن حجم سوق الذكاء الاصطناعي العالمي قد يتجاوز 2500 مليار دولار بحلول عام 2032، مع نمو سنوي مركب (CAGR)يزيد عن 19% خلال هذه الفترة.

- بين عامي 2022 و2023، نما حجم سوق الذكاء الاصطناعي العالمي بحوالي 84 مليار دولار (18.5%) ومن المتوقع أن ينمو بأكثر من 100 مليار دولار بحلول عام 2024.

ادوات ذكية في مجالات مختلفة

- https://zapier.com/blog/best-ai-productivity-tools/
- https://topai.tools/



تطبيقات الذكاء الاصطناعي

التحكم الآلي

تطوير الروبوتات والأنظمة الآلية القادرة على تنفيذ مهام تلقائيًا في مختلف المجالات.

أنظمة الدعم القرار

استخدام التحليلات المتقدمة والنماذج التنبؤية لدعم عملية اتخاذ القرار.

التوصيات الشخصية

تحليل البيانات الشخصية توصيات مخصصة في مجالات مثل الترفيه والتسوق.

التعرف على الأنماط

استخدام الذكاء الاصطناعي في مجالات مثل التصنيف والتعرف على الوجوه والكتابة اليدوية.

تطبيقات الذكاء الاصطناعي

الصناعة والتصنيع

يُطبق الذكاء الاصطناعي في الصناعة لتحسين كفاءة الإنتاج، وتحسين جودة المنتجات، وتخطيط وجدولة الإنتاج،

التعليم

يُساعد الذكاء الاصطناعي في تطوير أنظمة التعليم الشخصية، وإنشاء محتوى تعليمي تفاعلي، وتحليل بيانات الطلاب لتحسين

الصحة والرعاية الطبية

يُستخدم الذكاء الاصطناعي في مجال الرعاية الصحية لتحسين التشخيص الطبي، وتطوير أدوية جديدة، وتخطيط العلاجات،

بعض التطبيقات الحالية للذكاء الاصطناعي تغطي مجموعة واسعة من المجالات

الترفيه

- **تحليل المشاعر**: استخدام الذكاء الاصطناعي لتحليل ردود أفعال المشاهدين وتقديم توصيات لمحتوى يناسب اهتماماتهم.
- **إنشاء المحتوى**: تطوير أدوات تساهم في إنشاء محتوى إبداعي مثل النصوص، الموسيقى، والفيديوهات.
- **ألعاب الفيديو**: تحسين تجربة اللعب من خلال تطوير شخصيات ذكية وأنظمة لعب تتكيف مع أسلوب اللاعب

النقل

- **السيارات ذاتية القيادة**: تطوير سيارات قادرة على القيادة الذاتية باستخدام الذكاء الاصطناعي للتنقل بأمان على الطرق.
- **إدارة المرور**: استخدام الذكاء الاصطناعي لتحسين تدفق حركة المرور وتخفيض الازدحام من خلال التنبؤ بأنماط المرور وتوجيه السائقين.
- **اللوجستيات والشحن**: تحسين كفاءة سلاسل التوريد من خلال تحسين عمليات التخزين والنقل باستخدام الذكاء الاصطناعي.

التطبيقات الحالية للذكاء الاصطناعي تغطي مجموعة واسعة من المجالات

- **الزراعة**

- **الزراعة الدقيقة**: استخدام الطائرات بدون طيار وأجهزة الاستشعار لجمع البيانات حول المحاصيل وتحسين إدارة الموارد الزراعية.
- **مراقبة المحاصيل**: تحليل الصور الجوية للكشف عن الأمراض والآفات وتقديم توصيات للمزارعين.
- **تحسين الإنتاجية**: استخدام الذكاء الاصطناعي لتحليل البيانات الزراعية وتقديم توصيات لزيادة إنتاجية المحاصيل.

- **البيئات الذكية**

- **المنازل الذكية**: التحكم في الإضاءة، التدفئة، والأجهزة المنزلية باستخدام الذكاء الاصطناعي لتحسين كفاءة الطاقة والراحة.
- **المدن الذكية**: تحسين البنية التحتية والخدمات العامة من خلال تحليل البيانات وتقديم حلول مبتكرة لتحسين جودة الحياة.

بعض التطبيقات الحالية للذكاء الاصطناعي تغطي مجموعة واسعة من المجالات

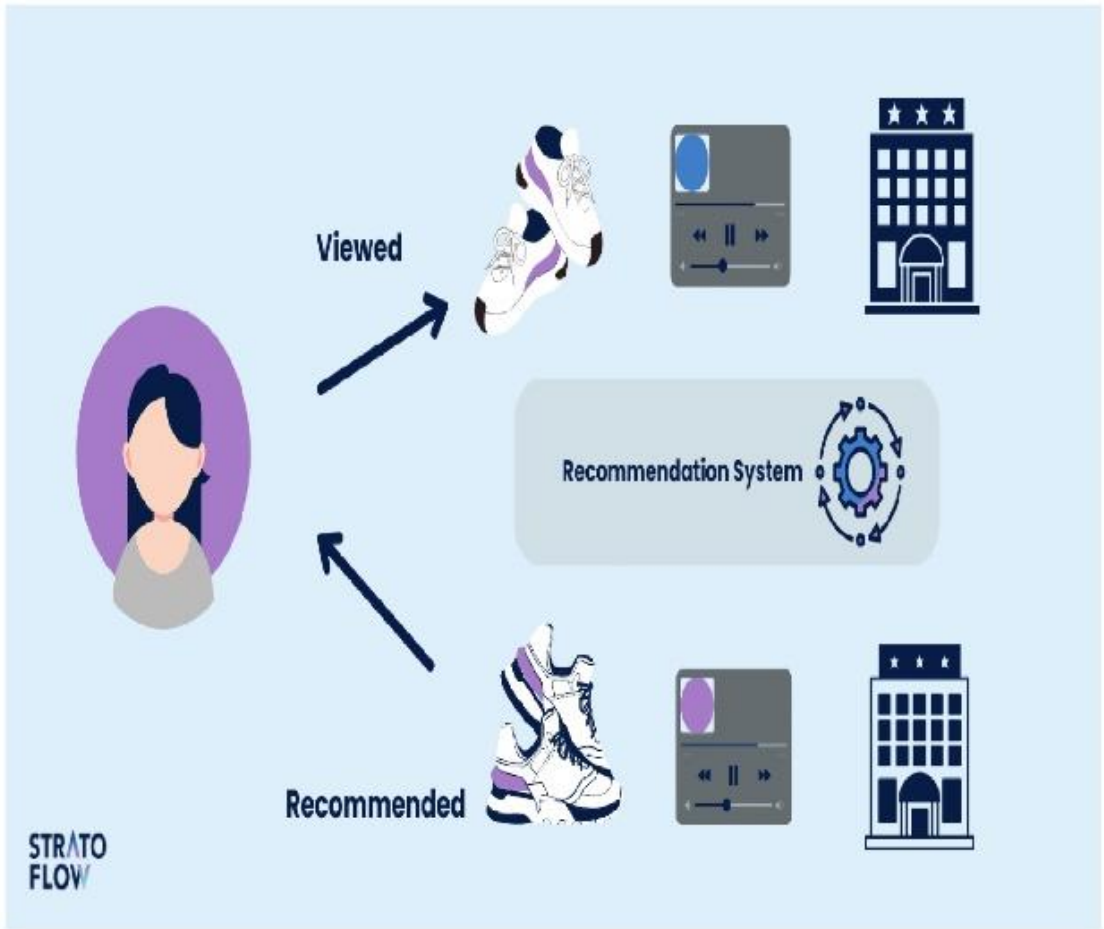
- **التجارة الإلكترونية**

- **توصيات المنتجات**: تحليل بيانات المستخدمين لتقديم توصيات مخصصة للمنتجات بناءً على سلوك الشراء السابق.
- **خدمة العملاء**: استخدام روبوتات الدردشة (Chatbots) لتحسين تجربة العملاء وتقديم الدعم على مدار الساعة.
- **إدارة المخزون**: توقع الطلبات المستقبلية وتحسين إدارة المخزون باستخدام خوارزميات الذكاء الاصطناعي.

- **الأمن السيبراني**

- **كشف التهديدات**: استخدام الذكاء الاصطناعي لتحليل الأنماط والكشف عن الأنشطة المشبوهة في الشبكات.
- **الاستجابة للحوادث**: تحسين سرعة الاستجابة للحوادث الأمنية من خلال التنبؤ بالتهديدات واتخاذ الإجراءات اللازمة تلقائيًا.
- **حماية البيانات**: تحسين أنظمة الحماية ومنع الاختراقات باستخدام تقنيات التعلم الآلي.

مثال على استخدام تعلم الآلة في الحياة اليومية:
خدمات التوصيات الشخصية



تقدم اقتراحات مخصصة للمستخدم بناءً على تفضيلاته وسلوكياته السابقة.
على سبيل المثال، خدمات البيع بالتجزئة الإلكترونية مثل أمازون و Netflix تستخدم تعلم الآلة لتوصية منتجات وأفلام وبرامج للمستخدم بناءً على سجل المنتجات والمحتوى التي تصفحها مسبقاً .

- **جمع البيانات:** تقوم هذه الخدمات بجمع بيانات عن تفضيلات المستخدم وأنماط تصفحه للمنتجات والمحتوى.
- **التحليل والتدريب**: تستخدم الخوارزميات الخاصة بتعلم الآلة لتحليل هذه البيانات وبناء نماذج تنبؤية عن ما قد يعجب المستخدم.
- **التوصيات الشخصية:** عندما يزور المستخدم الموقع، تقوم الخدمة بتوصية منتجات ومحتوى محتمل أن يعجبه بناءً على النماذج المتعلمة وهذا يحسن الحياة اليومية للمستخدمين من خلال تقديم توصيات شخصية مخصصة تلبي احتياجاتهم بشكل أفضل.

استخدام الذكاء الاصطناعي في تحسين إدارة الوقت وزيادة الإنتاجية

التنبؤ بالمهام والجداول الزمنية:

- يمكن لخوارزميات تعلم الآلة تحليل سجل الأنشطة والمواعيد السابقة للمستخدم.
- بناءً على ذلك، يمكنها التنبؤ بالمهام المتوقعة والوقت اللازم لإنجازها، وتقديم جداول زمنية مقترحة.
- هذا يساعد المستخدم على التخطيط أفضل لوقته والتنبؤ بالضغوطات في الجدول.

التنبيهات والتذكيرات الذكية:

- يمكن للأنظمة القائمة على تعلم الآلة تحليل عادات المستخدم وأنماط سلوكه.
- باستخدام هذه المعلومات، يمكنها تقديم تنبيهات وتذكيرات شخصية في الوقت المناسب للمهام المطلوبة.
- هذا يساعد المستخدم على البقاء منظمًا ويقلل من نسيان المهام الهامة.

إدارة المهام والأولويات:

- يمكن لأنظمة تعلم الآلة تحليل سجل إنجازات المستخدم والمهام المكتملة.
- باستخدام هذه البيانات، يمكنها اقتراح أولويات المهام والمساعدة في تخطيط وجدولة العمل بكفاءة أعلى.
- هذا يساعد المستخدم على التركيز على المهام الأكثر أهمية وتجنب التشتت.

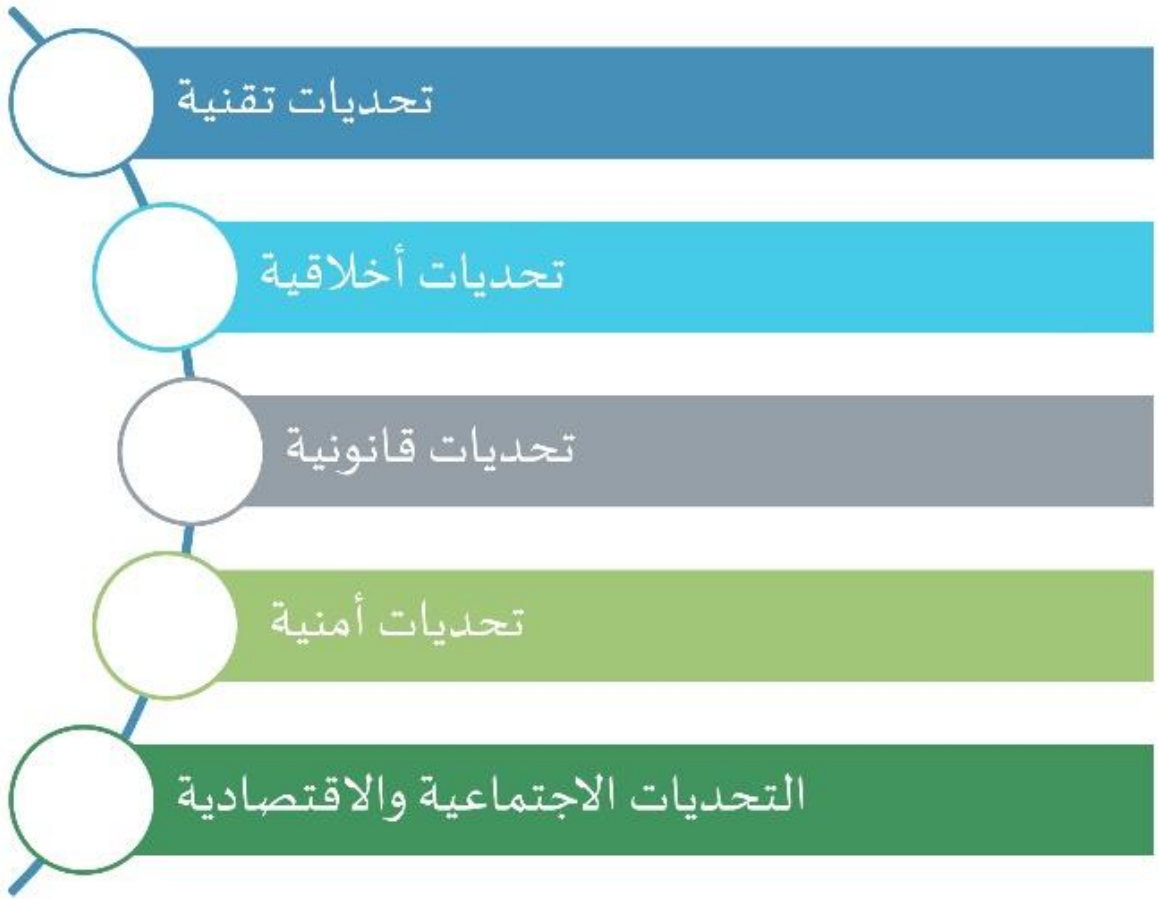
التحليلات الشخصية للإنتاجية:

- يمكن لتطبيقات تعلم الآلة تحليل نشاط المستخدم والبيانات المتعلقة به، مثل أنماط النوم وساعات العمل.
- باستخدام هذه التحليلات، يمكن تقديم توصيات شخصية لتحسين عادات العمل والحياة اليومية.
- هذا يمكّن المستخدم من فهم عاداته وتحسين إنتاجيته بطريقة مستدامة.

التحديات والمخاوف المرتبطة بالذكاء الاصطناعي

- الحاجة إلى كميات هائلة من البيانات لتدريب أنظمة التعلم الآلي بشكل فعال.
- الاعتبارات الأخلاقية والأمنية المرتبطة باستخدام الذكاء الاصطناعي في مهام حساسة.
- المخاوف من تأثير الذكاء الاصطناعي على سوق العمل وإمكانية استبدال البشر بالآلات.
- الحاجة إلى ضوابط وتشريعات لضمان تطوير الذكاء الاصطناعي بطريقة مسؤولة وآمن

التحديات في الذكاء الاصطناعي



- **الخصوصية والأمان**

حماية البيانات الشخصية ومنع الاختراقات.

- **الأخلاقيات**

ضمان استخدام التكنولوجيا بطرق أخلاقية ومسؤولة.

- **التحيز**

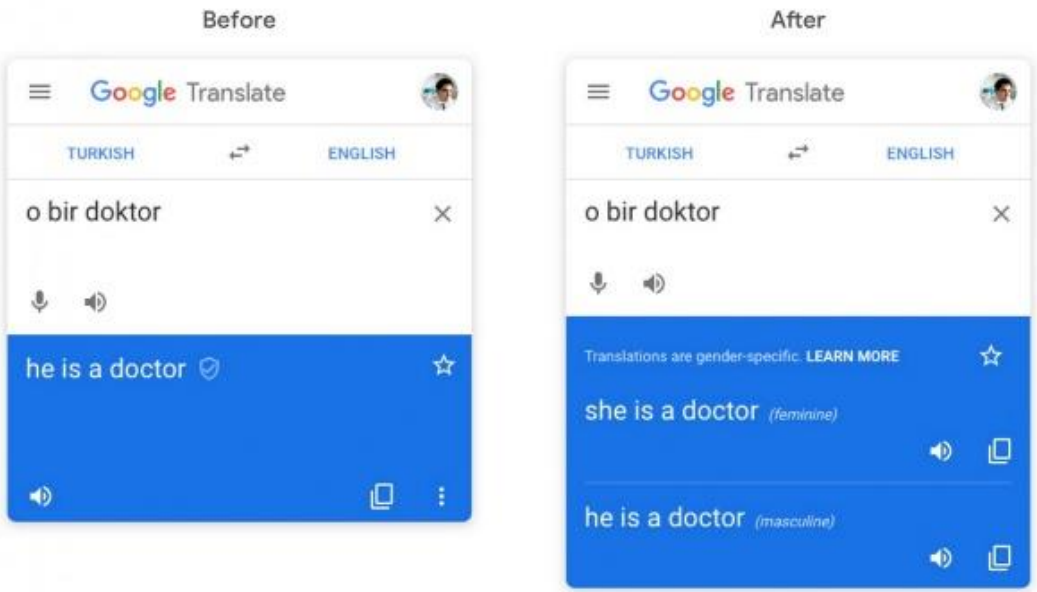
تجنب التحيز في البيانات والنماذج.

مثال على التحديات في الذكاء الاصطناعي

- في عام ٢٠١٢، حصل تطور كبير في مجال تصنيف الصور و التعرف على الكائنات بدقة عالية. هذا النجاح أدى الى اهتمام الكثير من الباحثين والشركات والمؤسسات في مجال الذكاء الصناعي. و تم استخدام تقنيات الذكاء الاصطناعي في مجال التعرف على الوجه بشكل واسع في مجالات عديدة .
- حدث هناك بعض الأخطاء والتي تم فيها مثلاً اتخاذ إجراءات قانونيه بناء على هذه الانظمة.
- ذلك أدى إلى التطرق الى المخاوف الأخلاقية المحتمل حدوثها في مجال الذكاء الاصطناعي وهي:

- الانحياز (Bias)
- الخصوصية والمراقبة (Privacy and Surveillance)
- الأتمتة و التوظيف (Automation and employment)
- المسؤولية (Accountability)

الانحياز في أنظمة الذكاء الاصطناعي



الانحيازفي ترجمة النصوص:

- بناء أنظمة منحازة إلي جنس دون الآخر في أنظمة ترجمة النصوص.

الانحيازفي أنظمة تحليل المشاعر:

- بناء أنظمة تحليل مشاعر منحازة تجاه عرق دون الآخر بحيث تختلف مخرجاتها باختلاف محتويات النص اذا ما احتوى نصوص عن عرق مختلف عن العرق السائد.

مستقبل الذكاء الاصطناعي

التوقعات والتحليلات

سيتمكن الذكاء الاصطناعي من إجراء توقعات دقيقة وتحليلات عميقة في مجالات مختلفة، مما سيحسن صنع القرار وحل المشكلات.

ابتكارات مستقبلية

يتوقع الخبراء أن يشهد الذكاء الاصطناعي تطورات مذهلة في المستقبل، بما في ذلك تحقيق الذكاء الاصطناعي العام (AGI)والذكاء الاصطناعي الفائق (ASI).

الاندماج مع الحياة اليومية

سيزداد استخدام الذكاء الاصطناعي في الأجهزة المنزلية والمكاتب

الذكاء الاصطناعي والبشرية

قد يؤدي تطور الذكاء الاصطناعي إلى تغييرات جذرية في طريقة عيش البشر وعملهم وتفاعلهم، مما يتطلب معالجة الجوانب الأخلاقية والاجتماعية.

مستقبل الذكاء الاصطناعي

سوق العمل والتوظيف

- أتمتة الوظائف: من المحتمل أن يؤدي الذكاء الاصطناعي إلى أتمتة العديد من الوظائف الروتينية، مما قد يقلل من الحاجة إلى العمالة البشرية في بعض المجالات ويزيد الطلب في مجالات أخرى.
- - فرص عمل جديدة: ستنشأ فرص عمل جديدة تتعلق بتطوير وصيانة أنظمة الذكاء الاصطناعي، مثل مهندسي البيانات ومتخصصي الأخلاقيات في الذكاء الاصطناعي.

التحديات والاعتبارات الأخلاقية

- الأمان والخصوصية: من الضروري معالجة المخاوف المتعلقة بأمان البيانات وخصوصية المستخدمين
- التحيز والإنصاف: يجب على المطورين التأكد من أن أنظمة الذكاء الاصطناعي غير متحيزة وتعامل جميع المستخدمين بعدالة.

البحث والتطوير

البحث المستمر: ستستمر الجامعات والمؤسسات البحثية في استكشاف مجالات جديدة في الذكاء الاصطناعي، مثل الذكاء الاصطناعي العاطفي والتعلم الفعّال.
التعاون بين البشر والآلات**: تطوير أنظمة الذكاء الاصطناعي التي تعمل بتكامل مع البشر ل لتحسين الإنتاجية وتوفير بيئات عمل أكثر أمانًا وفعالية.

مستقبل الذكاء الاصطناعي

معهد Stanford للذكاء الاصطناعي المرتكز على الإنسان (المصدر الأكثر ثقة في الاحصائيات وشموليتها) ينشر تقرير مؤشر الذكاء الاصطناعي لعام 2024.

التقرير يتحدث عن الذكاء الاصطناعي في التعليم والصناعة والصحة والكثير

مستقبل الذكاء الاصطناعي

معهد Stanford للذكاء الاصطناعي المرتكز على الإنسان (المصدر الأكثر ثقة في الاحصائيات وشموليتها) ينشر تقرير مؤشر الذكاء الاصطناعي لعام 2024.

التقرير يتحدث عن الذكاء الاصطناعي في التعليم والصناعة والصحة والكثير

الختمام

اتمنى لكم التوفيق والنجاح

م م عمر اياد