المركز الوطني
لتطوير المناهج
National Center
for Curriculum
Development

المهارات الرقمية

الصف التاسع - كتاب الطالب

الفصل الدراسي الثاني

9

لجنة الإشراف على التأليف

أ.د. وليد خالد سلامة
أ.د. باسل علي محافظة
أ.د. خالد إبراهيم العجلوني
ليلى محمد العطوي

هذا الكتاب جزء من مشروع الشباب والتكنولوجيا والوظائف لدى
وزارة الإقتصاد الرقمي والريادة.

الناشر: المركز الوطني لتطوير المناهج

يسر المركز الوطني لتطوير المناهج استقبال آرائكم وملحوظاتكم على هذا الكتاب عن طريق العناوين الآتية:

06-5376262 /237 | 06-5376266 | P.O.Box: 2088 Amman 11941
@nccdjor | feedback@nccd.gov.jo | www.nccd.gov.jo

قرَّرت وزارة التربية والتعليم تدريس هذا الكتاب في مدارس المملكة الأردنية الهاشـــمية جميعها، بناءً على قرار المجلس الأعلى للمركز الوطني لتطوير المناهج في جلســـته رقم (9/ 2024) تاريـــخ (30/ 10/ 2024) وقرار مجلس التربية والتعليم رقم (181/ 2024) تاريخ (17/ 11/ 2024) بدءًا من العام الدراسي (2024/ 2025).

ISBN 978-9923-41-723-2

المملكة الأردنية الهاشمية

رقم الإيداع لدى دائرة المكتبة الوطنية

(2024/10/5980)

المهارات الرقمية، الصف التاسع، الفصل الدراسي الثاني

تأليف/ هيئة: الأردن، المركز الوطني لتطوير للمناهج

عمان، المركز الوطني لتطوير للمناهج، 2024

رقم التصنيف: 373.19

المواصفات: / المهارات الحاسوبية/ / علم الحاسوب/ / المناهج/ / التعليم الأساسي/

يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعبر هذا المصنف عن دائرة المكتبة الوطنية.

فريق التأليف من شركة عالم الاستثمار للتنمية والتكنولوجيا

د. أسماء حسن حمدان　　د. محمد رجب عبدالمجيد　　د. رائد مصطفى القرعان

حنان حسني أبو راشد　　رهام صبحي الصالح

الطبعة الأولى (التجريبية)

1445هـ/ 2024م

المقدمة

انطلاقًا من إيمان المملكة الأردنية الهاشـــمية بأهمية تنمية قدرات الإنسان الأردني، وتسليحه بالعلم والمعرفة؛ ســـعى المركز الوطني لتطوير المناهج، بالتعاون مـــع وزارة التربية والتعليم، إلى تحديث المناهج الدراســـية وتطويرها، لتكون مُعينًا للطلبة على الارتقاء بمستواهم المعرفي والمهاري، ومجاراة أقرانهم في الدول المُتقدِّمة. ونظرًا إلى أهمية مبحث المهارات الرقميـــة ودوره في تنمية مهارات التفكير لدى الطلبة، وفتح آفاق جديدة لهم تُواكِب مُتطلَّبات ســـوق العمل؛ فقد أَوْلى المركز مناهجه عناية فائقة، وأَعدَّها وَفق أفضل الأســـاليب والطرائق المُتَّبَعة عالميًّا وأشرف عليها خبراء أردنيين؛ لضمان توافقها مع القِيَم الوطنية الأصيلة، ووفائها بحاجات الطلبة.

يُعَدُّ مبحث المهارات الرقمية واحدًا من أهمِّ المباحث الدراسية؛ إذ يُمثِّل الخطوة الأولى لتعريف الطلبة بمناحي التكنولوجيا والتطوُّر الرقمي الحديث بصورة موثوقة وآمنة. وقد اشتمل كتاب المهارات الرقمية على موضوعات تراعي التدرُّج في تقديم المعلومة، وعرضها بأســـلوب مُنظَّم وجاذب، وتعزيزها بالصور والأشـــكال؛ ما يُثْري المعرفة لدى الطلبة، ويُعزِّز رغبتهم في التعلُّم، ويُحفِّز هم على أداء أنشطة الكتاب المُتنوِّعة بيسر وسهولة، فضلًا عن تذكيرهم بالخبرات والمعارف التعليمية التي اكتسبوها سابقًا.
روعي في إعداد الكتاب الربط بين الموضوعات الجديدة على نحوٍ شامل ومُتكامِل، وتقديم موضوعاته بصورة شائقة تُعْنى بالســـياقات الحياتية التي تَهُمُّ الطلبة، وتزيد من رغبتهم في تعلُّم المهارات الرقمية. وقد أُلحِق بكل وحدة مقاطع تعليمية مُصوَّرة، تساعد الطلبة على الفهم العميق للموضوع، وتُرسِّخ لديهم ما تضمَّنه من معلومات وأفكار.

ونظرًا إلى ما تُمثِّله الأنشـــطة من أهمية كبيرة في فهم الموضوعات وتعزيـــز الطلاقة الإجرائية لدى الطلبة؛ فقد اشتمل الكتاب على أنشطة مُتنوِّعة تحاكي واقع الطلبة وما يحيط بهم، وتدعم تعلُّمهم، وتُثْري خبراتهم، فضلًا عن اشتماله على روابط إلكترونية يُمكِن للطلبة الاستعانة بها عند البحث في الأوعية المعرفية. ومن ثَمَّ، فإنَّ المهارات الرقمية والتقنية ترتبط ارتباطًا وثيقًا بمسيرة الطلبة التعليمية والمهنية.

ونحن إذ نُقدِّم هذا الكتاب، فإنَّنا نأمل أنْ يُســـهِم في بناء جيل واعٍ ومُبتكِر وقـــادر على التعامل مع التكنولوجيا بمسؤولية وإبداع، وأنْ يكون لَبِنة أساسية في تقدُّم المملكة الأردنية الهاشمية وازدهارها.

المركز الوطني لتطوير المناهج

الفهرس

دلالات أيقونات الكتاب

نشاط تمهيدي	نشاط استهلالي يربط التعلم السابق بالتعلم الحالي
نشاط عملي	نشاط تطبيقي مرتبط بمهارات الدرس
نشاط	نشاط مرتبط بمحتوى الدرس المعرفي أو المهاري
نشاط فردي	نشاط يطبق بشكل فردي
نشاط جماعي	نشاط يطبق في مجموعات
أبحث	أستخدم شبكة الإنترنت للبحث عن المعلومات

إثراء	توسع في المعلومات مرتبط بمحتوى الدرس
أناقش	عرض الأفكار وتبادلها مع الزملاء والمعلم
إضاءة	معلومة إضافية
أشاهد	عرض محتوى فيديو مرتبط بالمحتوى
مشروع	نشاط تكاملي توظف فيه معارف ومهارات الوحدة
مواطنة رقمية	الإجراءات الواجب اتباعها لتحقيق مبادئ المواطنة الرقمية
المهارات الرقمية	المهارات التكنولوجية التي سأطبقها في الوحدة

الوحدة
3

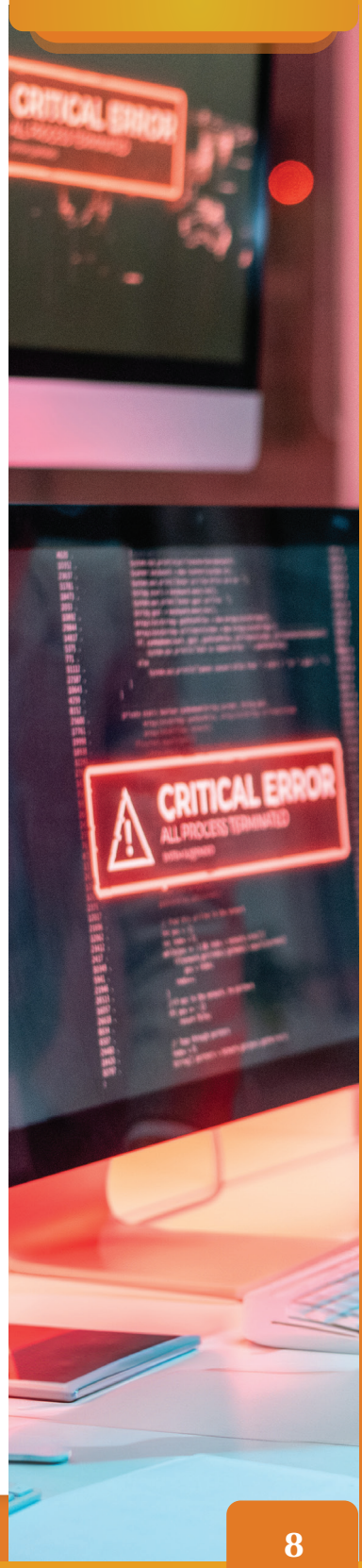
الأمنُ السيبرانيُّ (Cyber Security)

نظرةٌ عامّةٌ على الوَحْدة

تتناولُ الوحدةُ موضوعاتٍ أساسيةً في الأمنِ السيبرانيِّ وحمايةِ البياناتِ؛ حيثُ تبدأُ بتعريفِ مفهومِ حمايـــةِ البياناتِ وأمنِ المعلوماتِ وعناصرِهِ وركائزِهِ، ثمَّ تنتقلُ لتشرحَ تهديداتِ الأمنِ السيبرانيِّ، وكيفيةَ حمايةِ البياناتِ الشخصيةِ منَ التهديداتِ مثلَ البرمجياتِ الضارة وهجماتِ التصيُّدِ. تركزُ الوحدةُ أيضًا على وسائلِ الأمنِ الماديةِ والرَّقْميةِ، بما في ذلكَ استخدامُ الأقفالِ والأمانِ الفيزيائيِّ للحمايةِ منَ الوصولِ الماديِّ، بالإضافةِ إلى التشفيرِ والجدرانِ الناريةِ للحمايةِ الرقميةِ. وتُعنى أيضًا بكيفيةِ النقلِ الآمنِ للبياناتِ عبرَ الشبكةِ باتباعِ توصياتِ الأمنِ السيبرانيِّ، وتقدِّمُ نصائحَ حولَ وسائلِ حمايةٍ مختلفةٍ بناءً على الفعاليةِ والجدوى والأثرِ الأخلاقيِّ. أخيرًا، توضحُ الوحدةَ طرقَ التشـــفيرِ المختلفةَ، مثلَ التشفيرِ المتماثلِ وغيرِ المتماثلِ لضمانِ أمانِ البياناتِ.

يتوقعُ مني معَ نهايةَ الوحدةَ أنْ أكونَ قادرًا على:

- بيانِ مفهومِ حمايةِ البياناتِ.
- التمييزِ بينَ أمنِ البياناتِ والمعلوماتِ والأمنِ السيبرانيِّ.
- بيانِ عناصرِ أمنِ المعلوماتِ.
- بيانِ ركائزِ أمنِ المعلوماتِ.
- تطبيقِ كلماتِ سرٍّ قويةٍ واستخدامِها لحمايةِ الأجهزةِ والمعلوماتِ منَ الاستخدامِ غيرِ المصرحِ بهِ.
- توضيحِ مشكلاتِ الأمنِ السيبرانيِّ وطرقِ حمايةِ البياناتِ الشخصيةِ.
- استخدامِ وسائلِ الأمنِ الماديةِ والرقميةِ.
- توضيحِ طرقِ النقلِ الآمنِ للبياناتِ ونمذجتِها في الشبكةِ.
- اقتراحِ وسائلِ حمايةٍ عنْ طريقِ سيناريوهاتٍ مختلفةٍ ومقاييسَ محددةٍ، مثلَ الفعاليةِ والجدوى والتأثيراتِ الأخلاقيةِ لمشاركةِ البياناتِ.
- تطبيقِ عملياتِ التشفيرِ وفكِّ التشفيرِ باستخدامِ طرقٍ ومستوياتِ صعوبةٍ مختلفةٍ.



مَنتجاتُ التعلُّم (Learning Products)

حملةٌ إعلاميةٌ توعويةٌ للزملاءِ في المدرسةِ، تهدفُ إلى تعزيزِ وعيِهم بأهميةِ الأمنِ السيبرانيِّ وحمايةِ البياناتِ الشخصيةِ. مركزةٌ على أفضلِ الممارساتِ لحمايةِ الخصوصيةِ وأمانِ الحساباتِ عبرَ الإنترنتْ، وتوجيهِ الطلبةِ للتصرفِ بأمانٍ ووعيٍ في العالمِ الرقميِّ.

Google Docs

Google Slides

Genially

المهاراتُ الرَّقْميّةُ (Digital Skills): التفكيرُ الحاسـوبيُّ، البحثُ الرَّقْميّ، التواصلُ الرَّقْميّ، المواطنةُ الرَّقْميّةُ، الإدارةُ الذاتيةُ الرَّقْميّةُ، التعاونُ الرَّقْميُّ، الأمانُ الرَّقْميُّ.

مشروع

أختارُ معَ مجموعتيْ أحدَ المشـروعاتِ الآتيةِ للعمـلِ عليهِ بعدَ نهايةِ الوحدةِ:

المشـروعُ الأولُ: تصميمُ نموذجٍ بسـيطٍ لنظامِ أمانٍ رقميٍّ للمدرسةِ أوِ للمنزلِ، يسـاعدُ في فهمِ كيفيةِ حمايةِ المعلومـاتِ وتأمينِ البياناتِ باسـتخدامِ وسائلِ أمانٍ ماديةٍ ورقميةٍ، مثلَ اسـتخدامِ كلماتِ المرورِ، وتفعيلِ الجدُرِ الناريةِ وغيرِها.

المشروعُ الثاني: تطويرُ برنامجٍ باستخدامِ لغةِ سكراتش لمحاكاةِ فحصِ قوةِ كلمةِ مرورٍ مدخلةٍ، وتحديدِ معاييرِ القوةِ.

Coggle

Padlet

Canva

فهرسُ الوحدةُ

- **الدرسُ الأولُ**: أمنُ البياناتِ والمعلوماتِ (Data Information Security).
- **الدرسُ الثاني**: تهديداتُ الأمنِ السيبرانيِّ (Cyber Security Threats).
- **الدرسُ الثالثُ**: النقلُ الآمنُ للبياناتِ (Secure Data Transfer).
- **الدرسُ الرابعُ**: وسائلُ حمايةِ البياناتِ (Data Protection Means).
- **الدرسُ الخامسُ**: التشفيرُ (Encryption).

الدرسُ الأولُ

أمنُ البياناتِ والمعلوماتِ
(Data & Information Security)

مَنتجاتُ التعلُّمِ
(Learning Products)

فيديوهاتٌ توعويّةٌ عنْ أمنِ البياناتِ والمعلوماتِ ضمنَ الحملةِ التوعويّةِ لأفضلِ ممارساتِ الأمنِ السيبرانيِّ.

الفكرةُ الرئيسةُ

تعرُّفُ مفهومِ أمنِ البياناتِ والمعلوماتِ وعلاقتِهِ بالأمنِ السيبرانيِّ، وبيانُ عناصرِ أمنِ المعلوماتِ وركائزِهِ الثلاثةِ، وبيانُ أهميةِ كلماتِ المرورِ في حمايةِ البياناتِ والمعلوماتِ خاصةً البياناتِ الشخصيةَ، ومعرفةَ كيفيةِ اختيارِ كلماتِ سرٍّ قويةٍ وإدارتِها بشكلٍ صحيحٍ.

المفاهيم والمصطلحات

أمنُ البياناتِ (Data Protection).

الحرمانُ منَ الخدمةِ (Denial of Service – DoS).

الأمنُ السيبرانيُّ (Cyber Security).

أمنُ التطبيقاتِ (Application Security).

الأمنُ السحابيُّ (Cloud Security).

التّعافي من الكارثةِ (Disaster Recovery).

الاستجابةُ للحوادثِ (Incident Response).

أمنُ البنيةِ التحتيةِ (Infrastructure Security)

إدارةُ الثغراتِ الأمنيةِ (Vulnerability Management).

السِريَّةُ (Confidentiality).

النزاهة (Integrity)، التوافرُ (Availability).

إدارةُ الهُويّةِ والوصولُ (Identity and Access Management IAM).

المصادقةُ متعددةُ العواملِ (MFA)، كلماتُ السِّرِّ (Passwords).

نتاجات التعلُّم (Learning Outcomes)

- أميزُ بينَ أمنِ البياناتِ والمعلوماتِ والأمنِ السيبرانيِّ.
- أبينُ عناصرَ أمنِ المعلوماتِ.
- أبينُ ركائزَ أمنِ المعلوماتِ.
- أتعرَّفُ سببَ استخدامِ كلماتِ السرِّ لحمايةِ المعلوماتِ.
- أفرقُ بينَ كلمةِ السرِّ الضعيفةِ والقويةِ.
- أطبقُ طرقَ إنشاءِ كلماتِ سرٍّ قويةٍ .

في عصرِ الثورةِ الرقميةِ، أصبحتِ البياناتُ العصبَ الحيويَّ الذي يُغذي مختلفَ جوانبِ حياتِنا اليوميةِ، فعنْ طريقِ الهواتفِ الذكيةِ، والأجهزةِ المتصلةِ بالإنترنتْ، والتطبيقاتِ المتنوعةِ، ننتجُ كمياتٍ هائلةً منَ البياناتِ على نحوٍ مستمرٍّ. أدى هذا إلى ظهورِ مخاوفَ متعلقةٍ بحمايةِ البياناتِ. فما هيَ المفاهيمُ المرتبطةُ بأمنِ البياناتِ والمعلوماتِ؟

نشاط تمهيدي

أفكرُ في روتيني اليوميِّ، ثمَّ أذكرُ أمثلةً على البياناتِ التي أُنْتجُها، أوْ أتعاملُ معها. أيُّ هذهِ البياناتُ بحاجةٍ إلى حمايةٍ؟ ولماذا؟ هلْ سبقَ واستخدمتُ طرقًا أحمي بها بياناتِي؟ أذكرُها.

أناقشُ زملائِي بما توصلتُ إليهِ منْ أفكارٍ وأستمعُ إلى إجاباتِهمْ.

أمنُ البياناتِ والمعلوماتِ

تعرَّفْنا في صفوفٍ سابقةٍ مفهومَ البياناتِ وأشكالَها (كميةً أوْ نوعيةً، ملموسةً أوْ مجردةً، ثابتةً أوْ متغيرةً) وعلاقتَها بالمعلوماتِ. ونظرًا لأهميةِ المعلوماتِ في اتخاذِ القراراتِ، ظهرَ مفهومُ أمنِ المعلوماتِ الذي يشيرُ إلى مجموعةٍ منِ الإجراءاتِ والتدابيرِ الأمنيةِ التي تشملُ السياساتِ والإجراءاتِ والتقنياتِ التي تحمي المعلوماتِ الحساسةَ منْ سوءِ الاستخدامِ، أوِ الوصولِ غيرِ المصرحِ بهِ، أوِ التعطيلِ أوِ الإتلافِ. ويشملُ أمنُ المعلوماتِ الأمنَ الماديَّ والبيئيَّ والتحكُّمَ في الوصولِ، والأمنَ عبرَ الإنترنتْ.

أهمية أمن البيانات والمعلومات

وتبرزُ أهميَّةُ أمنِ المعلوماتِ في ما يأتي:

- **الحفاظِ على الخصوصيةِ:** يحمي أمنُ المعلوماتِ البياناتِ الشخصيةَ والحساسةَ منْ الوصولِ غيرِ المصرحِ بهِ؛ مما يحافظُ على خصوصيةِ الأفرادِ والمؤسساتِ.
- **ضمانِ النزاهةِ:** يمنعُ أمنُ المعلوماتِ التلاعبَ بالمعلوماتِ؛ مما يضمنُ أنْ تظلَّ دقيقةً وموثوقةً.
- **ضمانِ التوافرِ:** ضمانُ أنَّ المعلوماتِ متاحةٌ عندَ الحاجـــةِ إليها، معَ الحفاظِ على أنظمتِها منْ الهجماتِ التي قدْ تعطِّلُها، مثلَ هجماتِ الحرمانِ منِ الخدمةِ (DoS).
- **حمايةِ الأصولِ:** البياناتُ هيَ أحدُ أهمِّ الأصولِ لأيِّ مؤسسةٍ، ومنْ ثمَّ فإنَّ حمايتَها منِ الهجماتِ السيبرانيةِ والخروقاتِ الأمنيةِ أمرٌ بالغُ الأهميةِ.
- **الامتثالِ للقوانينِ:** هناكَ عديدٌ منْ القوانينِ والتشـــريعاتِ التي تلزمُ المؤسساتِ بحمايةِ بياناتِ العملاءِ، مثلَ اللائحـــةِ العامةِ لحمايةِ البياناتِ (General Data Protection Regulation: GDPR) وقانونِ حمايةِ خصوصيةِ المستهلكِ (Consumer Privacy Act: CCPA).

نشاط فردي

أبحثُ وأفكرُ في بنودٍ أخرى تبينُ أهميةَ أمنِ المعلوماتِ، معَ ذكرِ أمثلةٍ عليها، وأشاركُها معَ الزملاءِ في المجموعةِ الخاصةِ بالصفِّ، وأناقشُ زملائي بمشاركاتِهمْ.

علاقةُ أمنِ المعلوماتِ بالأمنِ السيبرانيِّ

الأمنُ السيبرانيُّ هوَ مجالٌ أوسعُ منْ أمنِ المعلوماتِ، ويرجعُ أصلُ مصطلحِ "الأمنِ السيبرانيِّ Cyber Security" الى كلمتيْ "الأمنِ" (Security) وتعني الحمايةَ أوِ الوقايةَ منَ الأخطارِ والتهديداتِ، وَ "Cyber" والتي تشيرُ إلى الفضاءِ الإلكترونيِّ أوِ الفضاءِ السيبرانيِّ الذي يشملُ الإنترنتْ والشبكاتِ الرقميةَ. بحيثُ يشـــملُ حمايةَ الأنظمةِ والشبكاتِ والأجهزةِ منَ الهجماتِ. ويركزُ على تأمينِ بيئةِ المعلوماتِ ضدَّ الهجماتِ منْ مصادرَ خارجيةٍ (مثلَ القراصنةِ)، ويتضمنُ جوانبَ مختلفةً، مثلَ أمنِ الشبكاتِ، وأمنِ التطبيقاتِ، وأمنِ السحابةِ، وأمنِ إنترنتْ الأشياءِ (IoT). ستتعلم المزيد عن الأمن السيبراني في الدروس اللاحقة.

يكمنُ الاختـــلافُ بينَ أمنِ المعلوماتِ والأمنِ الســـيبرانيِّ فـــي تركيزِ أمنِ المعلوماتِ بشكلٍ أساسيٍّ على حمايةِ البياناتِ والمعلوماتِ بغضِّ النظرِ عنْ مكانِها (ســـواءٌ أكانتْ على الورقِ أوْ في الأنظمةِ الرقميةِ)، أما الأمنُ السيبرانيُّ، فيركزُ على حمايةِ الأنظمةِ والشبكاتِ في الفضاءِ السيبرانيِّ.

نشاط جماعي

أحلِّلُ وأصنفُ

أتعاونُ معَ الزملاءِ في المجموعةِ لدراســـةِ الحالاتِ الآتيةِ، وتصنيفِها إلى أمنِ معلوماتٍ أوْ أمنٍ سيبرانيٍّ:

- استخدامُ جدارٍ ناريٍّ لحمايةِ شبكةِ الشركةِ منَ الهجماتِ الخارجيةِ.
- قيامُ الموظفِ بتشفيرِ ملفٍّ يحتوي على بياناتٍ حساسةٍ قبلَ مشاركتِهِ عبرَ البريدِ الإلكترونيِّ.
- اكتشافُ نظامِ كشفِ التسللِ نشاطًا مشبوهًا في شبكةِ المدرسةِ، وتمَّ إيقافُهُ فورًا.
- تثبيتُ برنامجِ مكافحةِ الفيروساتِ على جميعِ أجهزةِ الكمبيوترِ لحمايتِها منَ البرمجياتِ الخبيثةِ.
- إنشاءُ كلمةِ مرورٍ قويةٍ لحسابِهِ الشخصيِّ على موقعِ الخدماتِ المصرفيةِ عبرَ الإنترنتْ.
- تحذيرُ الشركةِ موظفيها منْ فتحِ رسائلِ البريدِ الإلكترونيِّ المشبوهةِ التي قدْ تحتوي على برمجياتٍ خبيثةٍ.
- نَسخُ البياناتِ المهمةِ للشركةِ احتياطيًّا على خادمٍ آمنٍ في حالةِ حدوثِ خللٍ تِقنيٍّ.
- تطبيقُ المصادقةِ الثنائيةِ على حساباتِ المستخدمينَ لتوفيرِ طبقةٍ إضافيةٍ منَ الحمايةِ.
- تحديثُ نظامِ التشغيلِ على جميعِ الأجهزةِ لضمانِ الحمايةِ منَ الثغراتِ الأمنيةِ.
- تحديدُ سياسةِ استخدامٍ آمنةٍ لوسائلِ التواصلِ الاجتماعيِّ لموظفي الشركةِ.

نعرضُ ما توصلنا إليهِ منْ تصنيفاتٍ على مستوى المجموعةِ، ونبرِّرُ تصنيفاتِنا، ونناقشُ الزملاءَ فيها ونستمعُ إلى آرائِهمْ.

العناصرُ الرئيسةُ لسياسةِ أمنِ المعلوماتِ والأمنِ السيبرانيِّ

تضمُّ سياسةُ أمنِ المعلوماتِ والأمنِ السيبرانيِّ مجموعةَ أدواتِ الأمانِ، وحلولِهِ وعملياتِهِ التي تحافظُ على أمانِ معلوماتِ الأفرادِ والمؤسساتِ عبرَ الأجهزةِ والمواقعِ والشبكاتِ والأنظمةِ السحابيةِ؛ مما يساعدُ على الحمايةِ منَ الهجماتِ الإلكترونيةِ أوِ الأحداثِ التخريبيةِ الأخرى.

1. **أمنَ التطبيقاتِ (Application Security)**: النهجُ والإجراءاتُ والأدواتُ وأفضلُ الممارساتِ التي توضعُ لحمايةِ التطبيقاتِ وبياناتِها. يمكنُ استخدامُ أدواتِ فحصِ الثغراتِ، مثلَ Burp Suite.

2. **الأمنَ السحابيَّ (Cloud Security)**: النهجُ والإجراءاتُ والأدواتُ وأفضلُ الممارساتِ التي توضعُ لحمايةِ السحابةِ ككلٍّ، بما في ذلكَ الأنظمةُ والبياناتُ والتطبيقاتُ والبنيةُ الأساسيةُ. ويتضمنُ تشفيرَ البياناتِ، والتحكمِ في الوصولِ، ومراقبةَ الأنشطةِ عبرَ السحابةِ.

3. **التّعافي منَ الكارثةِ (Disaster Recovery)**: طريقةٌ لإعادةِ إنشاءِ أنظمةٍ تكنولوجيةٍ فعالةٍ في أعقابِ حدثٍ، مثلَ كارثةٍ طبيعيةٍ أوْ هجومٍ إلكترونيٍّ أوْ حدثٍ تخريبيٍّ آخرَ. ويتضمنُ تطويرَ خطةِ التعافي منَ الكوارثِ والنسخِ الاحتياطيِّ المنتظمِ للبياناتِ.

4. **الاستجابةَ للحوادثِ (Incident Response)**: خطةٌ للاستجابةِ لتداعياتِ أيِّ هجومٍ عبرَ الإنترنتْ أوْ تسربٍ للبياناتِ أوْ حدثٍ تخريبيٍّ آخرَ، ومعالجتِهِ وإدارتِهِ. ويتضمنُ استخدامَ أدواتِ تحليلِ الأمانِ، مثلَ نظامِ إدارةِ المعلوماتِ والأحداثِ الأمنيةِ (SIEM) لرصدِ الحوادثِ الأمنيةِ وتحليلِها.

5. **أمنَ البنيةِ التحتيةِ (Infrastructure Security)**: الأمانُ الذي يشملُ البنيةَ التحتيةَ التكنولوجيةَ، بما في ذلكَ أنظمةُ الأجهزةِ والبرامجِ. ويتضمنُ تأمينَ الشبكةِ وتحديثَ الأنظمةِ بانتظامٍ وتطبيقَ قواعدِ التحكمِ في الوصولِ.

6. **إدارة الثغرات الأمنية (Vulnerability Management)**: العملية التي تجريها المؤسسة لتحديد الثغرات الأمنية في نقاط النهاية والبرامج والأنظمة الخاصة بها، وتقييمها ومعالجتها.

أبحث

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنْ إجـــراءاتِ الأمانِ التي يمكنُ تطبيقُها في نظامِ التشغيلِ ويندوز (Windows)، ثمَّ أجهزُ عرضًا تقديميًا عنْ هذهِ الإجراءاتِ باستخدامِ (Google Slides)، معَ إرفاقِ الصورِ والفيديوهاتِ التوضيحيةِ، وأشـــاركُهُ على اللوحِ التفاعليِّ الرقميِّ للصفِّ.

نشاط جماعي

أناقـــشُ معَ زملائِي في المجموعةِ إجراءاتِ الأمانِ التي يمكـــنُ تفعيلُها على الهواتفِ الذكيةِ، وندونُ مقترحاتِنا معَ ذكرِ نظامِ التشغيلِ المستهدفِ (مثلَ أندرويد، iOS) ونتشاركُ الأفكارَ معَ المجموعاتِ الأخرى، وندونُ أفكارًا جديدةً تعلمْناها منهمْ.

إثراء

BitLocker Drive Encryption: هوَ أداةُ تشـــفيرٍ منْ مايكروســـوفت، تقومُ بتشفيرِ محركاتِ الأقراصِ بالكامـــلِ على نظامِ ويندوز. تُســـتخدمُ هذهِ الميـــزةُ لضمانِ أمـــانِ البياناتِ منَ الســـرقةِ أوَ الوصولِ غيرِ المصرحِ بهِ، حتى في حالِ فقدانِ أوْ ســـرقةِ جهـــازِ الكمبيوترِ. يقومُ BitLocker بتشـــفيرِ كلِّ محتوياتِ محركِ الأقراصِ باســـتخدامِ خوارزمياتِ تشفيرٍ قويةٍ، مثلَ (AES–Advanced Encryption Standard) بأطـــوالِ مفاتيحَ تصلُ إلـــى 256 بت. هذا يعني أنَّ البياناتِ المخزنةَ على محركِ الأقراصِ تُحـــولُ إلى صيغةٍ غيرِ قابلةٍ للقراءةِ منْ دونِ مِفتاحِ فكِّ التشفيرِ الصحيحِ. يحتاجُ المستخدمُ إلى تقديمِ مِفتاحِ فكِّ التشفيرِ للوصولِ إلى البياناتِ. يمكنُ أنْ يكونَ هذا المفتاحُ كلمةَ مرورٍ، أوْ بطاقةً ذكيةً، أوْ بصمةَ الإصبعِ.

الركائزُ الثلاثُ لأمنِ المعلوماتِ (السِريَّةُ، والنزاهة، والتوافرُ)

تمثلُ عناصرُ "السريةِ" و"النزاهة" و"التوافرِ" الركائزَ الأساسيةَ لأنظمةِ حمايةِ المعلوماتِ (الشكلِ 1-1)، التي تشكلُ البنيةَ الأساسيةَ الأمنيةَ للمؤسساتِ. وتعدُّ هذهِ العناصرُ المبادئَ التوجيهيةَ لتنفيذِ أيِّ خطةٍ لأمنِ المعلوماتِ.

الشكل (1-1): الركائز الثلاث لأمن المعلومات

في ما يأتي توضيحٌ لكلٍّ منها:

1. **السِريَّةُ (Confidentiality):**

تمثلُ السِريَّةُ مكونًا رئيسًا لأمنِ المعلومات، ويجبُ وضعُ إجراءاتٍ تسمحُ فقطْ للمستخدمينَ المصرَّحِ لهمْ بالوصولِ إلى المعلوماتِ. يمثلُ تشفيرُ البياناتِ (Encryption) والمصادقةُ متعددةُ العواملِ (MFA) وكلماتُ المرورِ (Passwords) جزءًا منَ الأدواتِ التي يمكنُ استخدامُها للمساعدةِ في ضمانِ سِريَّةِ البياناتِ

2. **النزاهةُ (Integrity):**

تعني النزاهةُ (السلامةُ) الحفاظَ على صحةِ المعلوماتِ ودقتِها، وعدمَ تعديلِها أوِ التلاعبِ بها بطرقٍ غيرِ شرعيةٍ، والتأكدَ منْ أنَّ البياناتِ تظلُّ كاملةً وصحيحةً منذُ إنشائِها حتى الوصولِ إليها. تساعدُ أدواتٌ مثلُ أذوناتِ الوصولِ إلى الملفاتِ (Access Permissions)، وإدارةِ الهُويةِ، والتحكمِ في الوصولِ (Identity and Access Management – IAM) في ضمانِ نزاهةِ البياناتِ.

3. **التوافرُ (Availability):**

يشيرُ التوافرُ إلى ضمانِ وصولِ المعلوماتِ والخدماتِ إلى المستخدمينَ المصرَّحِ لهم عندما يحتاجونَ إليها؛ أيْ أنَّ النظامَ والخدماتِ تعملُ بشكلٍ صحيحٍ، ويمكنُ الوصولُ إليها عندَ الحاجةِ. تتضمنُ سياسةُ أمانِ المعلوماتِ صيانةَ الأجهزةِ الماديةِ باستمرارٍ، واستكمالَ ترقياتِ النظامِ بانتظامٍ؛ لضمانِ حصولِ المستخدمينَ المعتمدينَ على وصولٍ متسقٍ، يمكنُ الاعتمادُ عليهِ في البياناتِ التي يحتاجونَ إليها.

نشاط جماعي

محاكاةُ ركائزِ أمنِ المعلوماتِ (Confidentiality, Integrity, Availability: CIA)

أتعاونُ معَ الزملاءِ في المجموعةِ على محاكاةِ ركائزِ أمنِ المعلوماتِ بتنفيذِ الخطواتِ الآتيةِ:

1. **السِريَّةُ:**

حمايةُ المستنداتِ :

- أنشئُ مستندًا يحتوي معلوماتٍ حساسةً (مثلَ بياناتٍ ماليةٍ أوْ معلوماتٍ شخصيةٍ).
- **تشفيرُ المستندِ:** أعملُ على تشفيرِ المستندِ باستخدامِ أدواتِ التشفيرِ المتاحةِ في نظامِ التشغيلِ (Windows).

(بالنقرِ على المجلدِ بالزرِ الأيمنِ، ثمَّ اختيـــارُ –خصائص– ومنْ تبويب عام، نختارُ متقدم، ثمُّ نختارُ "تشفير محتوى المجلد")

- **اختبارُ الوصولِ:** أُجري اختبارَ الوصولِ إلى المستنداتِ المُشفَّرةِ.

2. **النزاهة:**

توقيعُ المستندِ رقميًّا:

- استخدامُ التوقيعِ الرَّقْميِّ لحمايةِ المستنداتِ منَ التلاعبِ. (أحفظُ الملفُ بصيغةِ (PDF)، ثمَّ أفتحُهُ باستخدامِ برنامجِ (Acrobat Reader)، وأضيفُ التوقيعَ منَ الأدواتِ المتوافرةِ).

3. **التوافرُ:**

عملُ نسخةٍ احتياطيّةٍ:

- أعملُ نسخةً احتياطيةً منَ المستنداتِ الحساسةِ باستخدامِ أدواتِ النسخِ الاحتياطيِّ المتاحةِ (مثلِ خدماتِ التخزينِ السحابيِّ Google Drive).
- **اختبارُ الاستعادةِ:**
- أجري اختبارًا لاستعادةِ النُّسخِ الاحتياطيةِ للتحققِ منْ أنّها تعملُ بشكلٍ صحيحٍ، ويمكنُ استعادةُ المستنداتِ عندَ الحاجةِ.
- **إنشاءُ خُطةٍ للطوارئِ:**
- أُعِدُّ خطةً للطوارئ، تتضمنُ خطواتٍ لاستعادةِ الوصولِ إلى المستنداتِ الحساسةِ في حالِ فقدانِ البياناتِ أوْ تلفها.

نتبادلُ الخبراتِ معَ المجموعاتِ الأُخرى، ونتشـــاركُ في فحصِ الملفـــاتِ للتأكدِ منْ صحةِ إجراءاتِ الأمانِ.

استخدامُ كلماتِ السِّرّ لحمايةِ البياناتِ

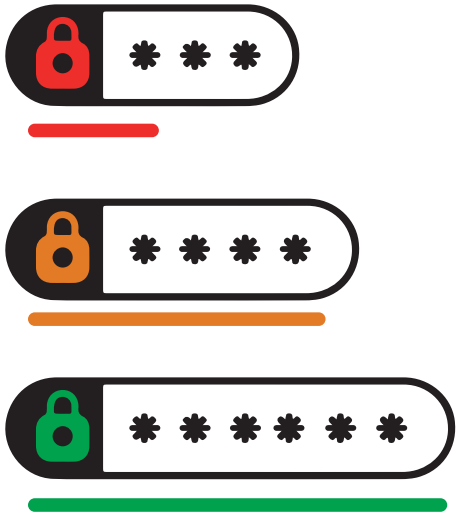
أبحثُ

أستخدمُ المواقعَ الإلكترونيةَ الموثوقةَ للبحثِ عنِ الأسبابِ التي جعلتْ كلمةَ السرِّ أكثرَ طرقِ حمايةِ البياناتِ انتشارًا. ثمَّ أشاركُ ما أتوصلُ إليهِ معَ الزملاءِ على اللوحِ الرقميِّ التفاعليِّ للصفِّ.

تعدُّ كلماتُ السرِّ أوْ كلماتُ المرورِ (Passwords) منْ أكثرِ طرقِ حمايةِ البياناتِ شيوعًا خاصةً في حمايةِ البياناتِ الشخصيةِ، وتبرزُ أهميتُها في منعِ الوصولِ غيرِ المصرحِ بهِ للبياناتِ أوِ المعلوماتِ، وحمايةِ البياناتِ الحساسةِ، وتعزيزِ الخصوصيةِ الشخصيةِ، وحمايةِ الأجهزةِ والشبكاتِ، وهيَ عنصرٌ أساسيٌّ في استراتيجياتِ الأمانِ متعددةِ الطبقاتِ. وتكمنُ أهميتُها في بيئاتِ العملِ بحمايةِ البياناتِ الحساسةِ للعملاءِ، وحمايةِ الأصولِ الرقميةِ.

نبينُ في ما يأتي أفضلَ الممارساتِ لاستخدامِ كلمةِ السِّرِّ لحمايةِ أمنِ البياناتِ والمعلوماتِ:

1. **إنشاءُ كلماتِ سرٍّ قويّةٍ:** تُحدَّدُ قوةُ كلماتِ المرورِ بما يأتي:
   - **الطولِ:** يجبُ أنْ تكونَ كلمةُ السرِّ طويلةً، تكونُ -عمومًا- أثني عشرَ حرفًا أوْ أكثرَ.
   - **التعقيدُ:** يجبُ أنْ تتضمنَ مزيجًا منَ الحروفِ الكبيرةِ والصغيرةِ، والأرقامِ، والرموزِ الخاصةِ.
   - **التنوعُ:** تجنُّبُ استخدامِ كلماتِ السِّرِّ البسيطةِ أوِ الشائعةِ، مثلَ "password123".



2. **تغييرُ كلماتِ السِّرِّ بانتظامٍ:** يجبُ تحديثُ كلماتِ السِّرِّ بشكلٍ دوريٍّ؛ لتقليلِ المخاطرِ إذا اكتُشِفتْ كلمةُ السرِّ القديمةِ.
3. **عدمُ استخدامِ كلماتِ سرٍّ متكررةٍ:** لا تستخدمْ كلمةَ السرِّ نفسَها لحساباتٍ متعددةٍ؛ لتقليلِ المخاطرِ في حالِ اختُرِقَ أحدُ الحساباتِ.
4. **المحافظةِ على سريةِ البياناتِ:** عدمُ كتابةِ كلمةِ السَّرِّ على ورقةٍ خارجيةٍ والاكتفاءُ بحفظِها في الذاكرةِ.

إضاءةٌ

وفقًا لتقريرِ تحقيقاتِ خرقِ البياناتِ لعامِ 2020 من Verizon، فإنَّ 81٪ منْ حالاتِ الاختراقِ المرتبطةِ بالقرصنةِ ناتجةٌ عنْ كلماتِ مرورٍ مسروقةٍ أوْ ضعيفةٍ.

وفي دراسةٍ أجراها المركزُ الوطنيُّ للأمنِ السيبرانيِّ في المملكةِ المتحدةِ (NCSC) عامَ 2019، عُثرَ على 23.2 مليونَ حسابِ ضحيةٍ حولَ العالمِ، استخدموا كلمةَ المرورِ "123456".

أبحث

أبحثُ باستخدامِ محركِ البحثِ عنْ أكثرِ كلماتِ السرِّ استخدامًا لعامِ 2024. ماذا أستنتجُ منْ ذلكَ؟ أقدمُ مقترحاتٍ لحمايةِ كلمةِ المرورِ الخاصةِ بي، وأشاركُ أفكاريَ معَ الزملاءِ.

نشاط عملي

أحكمُ على كلماتِ المرورِ الخاصةِ بي ومدى قوَّتِها باستخدامِ الموقعِ الآتي:

https://www.security.org/how-secure-is-my-password/

ملحوظةٌ: للحفاظِ على الخصوصيةِ، يمكنُ استخدامُ كلماتِ مرورٍ وهميةٍ تحاكي كلمةَ المرورِ الخاصةِ بي منْ حيثُ عددُ الرموزِ وطبيعتِها.

إضاءةٌ

تزدادُ شعبيةُ أنظمةِ الدخولِ منْ دونِ كلمةِ سرٍّ (Password-less Systems) بسببِ الأمانِ المحسَّنِ، وتجربةِ المستخدمِ المحسَّنةِ التي توفرُها. تقدمُ هذهِ الأنظمةُ مجموعةً متنوعةً منَ الطرقِ للتحققِ منْ هُويةِ المستخدمينَ بشكلٍ آمنٍ منْ دونِ الاعتمادِ على كلماتِ السرِّ التقليديةِ. ومعَ تقدمِ التكنولوجيا، يُتوقعُ أنْ تصبحَ المصادقةُ منْ دونِ كلمةِ سرٍّ هيَ القاعدةُ الأساسيةُ في الأمانِ الرقميِّ.

نشاط فردي

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنْ تأثيرِ الـــذكاءِ الاصطناعيِّ في أمنِ المعلوماتِ وكلماتِ المرورِ. وأكتبُ فقرةً حولَ ذلكَ، وأشاركُها معَ الزملاءِ عبرَ اللوحِ الرقميِّ التفاعليِّ، وأستطلعُ مشاركاتِهمْ وأتفاعلُ معها وأناقشُهمْ فيها.

المواطنةُ الرقميةُ

- **الوعيُ والمسؤوليةُ**: المسؤوليةُ الشخصيةُ عندَ استخدامِ الإنترنت باستخدامِ كلماتِ مرورٍ قويةٍ، والالتزامُ بحمايةِ نفسي والآخرينَ منْ المخاطرِ الرقميةِ.
- **الأمانُ الشخصيُّ والمجتمعيُّ**: تبني ممارســـاتِ أمانِ البياناتِ، ومراجعةُ الأذوناتِ بعنايةٍ قبلَ تحميلِ التطبيقاتِ، خاصةً تلكَ غيرَ المعروفةِ أوِ التـــي لا تبدو موثوقةً. عدمُ النقرِ على روابطَ مشبوهةٍ أوْ تقديمُ معلوماتٍ حساسةٍ عندَ الطلبِ عبرَ البريدِ الإلكترونيِّ أوْ الرسائلِ النصيةِ؛ مما يسهمُ في تعزيزِ الأمانِ الرقميِّ للفردِ والمجتمعِ.
- **الخصوصيةُ الرقميةُ**: تطبيقُ إجراءاتِ أمنِ المعلوماتِ لحمايةِ البياناتِ الشخصيةِ منَ الاختراقِ أوَ التلاعبِ. والحفاظُ على الخصوصيةِ عندَ استخدامِ الإنترنتْ، وتجنُّبُ الإفصاحِ عنْ معلوماتٍ حساسةٍ في الأماكنِ العامةِ أوْ على الشبكاتِ غيرِ الآمنةِ.

مشروع

المشروعُ: حملةٌ إعلاميةٌ توعويةٌ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ/ مهمةُ 1

أتعاونُ معَ زملائِي لإنتاجِ أولِ مهمةٍ في الموادِّ التوعويةِ التي تتمحورُ حولَ إنتاجِ فيديو توعويٍّ عنْ أمنِ البياناتِ والمعلوماتِ باتباعِ الخطواتِ الآتيةِ:

1. **أحددُ الموضوعَ الأساسيَّ** للفيديو مثلَ "أمنِ المعلوماتِ وأهميتِهِ وعلاقتِهِ بالأمنِ السيبرانيِّ" و"كلماتِ المرورِ وطريقةِ إنشائِها وأهميةِ كلماتِ المرورِ القويةِ"..
2. **اكتبْ سيناريو شاملًا**، يتضمنُ معلوماتٍ دقيقةً ومشوقةً.
3. **جمعُ الواردِ:** أستخدمُ صورًا عاليةَ الجودةِ وفيديوهاتٍ إضافيةً إنْ لزمَ، وأجهزُ النصوصَ التي ستعرضُ على الشاشةِ، أوْ تسجَّلُ صوتيًا.
4. **التسجيلُ والتحريرُ:** أستخدمُ Video Editor لإضافةِ الصورِ، والفيديوهاتِ، والنصوصِ، وأضيفُ الموسيقى أوِ الصوتِ التعليميَّ إذا تطلبَ الأمرُ.
5. **التحسينُ والتصميمُ:** أتأكدُ منْ وضوحِ المعلوماتِ، وأنظمُ محتوى الفيديو بحيثُ يكونُ جذابًا.
6. **المراجعةُ:** أختبرُ الفيديو للتأكدِ منْ الترتيبِ والدقةِ، وأعدلُ الفيديو إذا لزمَ الأمرُ؛ لتحسينِ الجاذبيةِ والتنظيمِ.

أراعي عندَ عملَ الفيديوهات:

- الدقة والوضوحُ؛ دقةُ المعلوماتِ المعروضةِ في الفيديو ووضوحُها.
- التصميم؛ تصميمُ جذابٍ ومشوقٍ.
- استخدام صورٍ عاليةِ الدقةِ.
- الترتيبَ والتنظيمَ.
- مناسبةَ وقتِ الفيديو للمحتوى.

أقيِّم تعلُّمي

المعرفةُ: استخدمُ ما تعلمتَهُ منْ معارفَ في هذا الدرسِ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: أقارنُ بينَ أمنِ المعلوماتِ والأمنِ السيبرانيِّ.

.....

.....

السؤالُ الثاني: أبيّنُ العناصرَ الرئيسةَ لسياسةِ أمنِ المعلوماتِ.

.....

السؤالُ الثالثُ: أوضحَ أهميةَ استخدامِ كلماتِ المرورِ لحمايةِ البياناتِ الشخصيةِ.

.....

المهاراتُ: أوظفُ مهاراتِ التفكيرِ الناقدِ، والبحثِ الرقميِّ، والتواصلِ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: أبحثُ في طرقِ الحفاظِ على أمنِ المعلوماتِ الحديثةِ، وأدونُها في مستندِ Google Docs.

.....

.....

السؤالُ الثاني: أفكرُ في طرقٍ برمجيةٍ لإنشاءِ كلماتِ المرورِ وتغييرِها بشكلٍ دوريٍّ.

.....

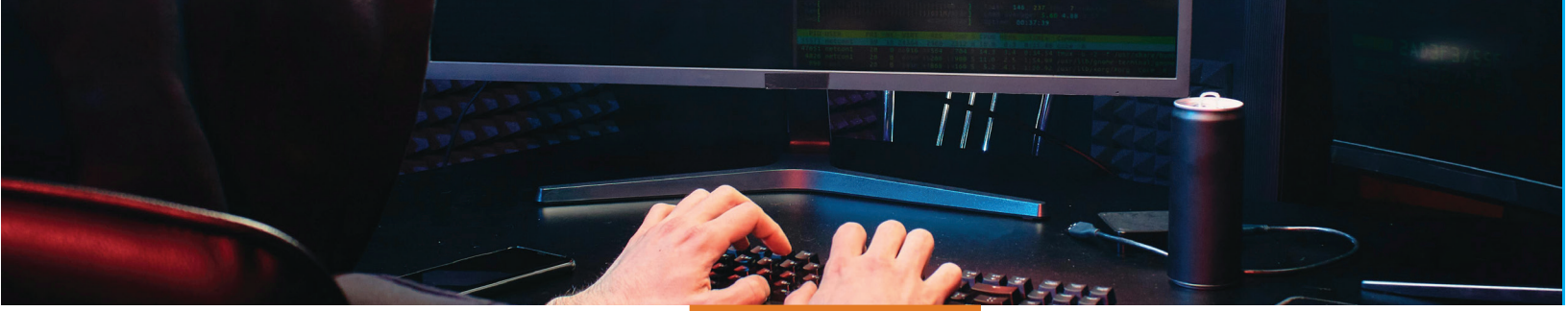
.....

السؤالُ الثالثُ: هلْ أتوقعُ أنْ تكونَ المعلوماتُ في المستقبلِ الرقميِّ وتطوراتِهِ المتسارعةِ أكثرَ أمانًا؟ أفسرُ إجابتِي.

.....

قِيَمٌ واتجاهاتٌ

أتعاونُ معَ الزملاءِ لتصميمِ إنفوجرافيك يبينُ ممارساتِ المواطنةِ الرقميةِ المتعلقةِ بأمنِ البياناتِ، وأنشرُهُ على الموقعِ الإلكترونيِّ للمدرسةِ.



الدرس الثاني

تهديداتُ الأمنِ السيبرانيِّ
(Cyber Security Threats)

الفكرةُ الرئيسةُ

التعرُّفُ إلى مفاهيمِ الأمنِ السيبرانيِّ ومشكلاتِهِ، وتوضيحُ طرقِ حمايةِ البياناتِ الشخصيةِ باستخدامِ وسائلِ الحمايةِ الماديةِ والرقميةِ، واستكشافُ أمثلةٍ واقعيةٍ تتعلقُ بالأمنِ السيبرانيِّ.

المفاهيم والمصطلحات

تهديداتُ الأمنِ السيبرانيِّ (Cyber Security Threats)،
الهجماتُ الإلكترونيةُ (Cyber Attacks)،
الاعتداءُ الإلكترونيُّ (Cyber Assault)،
التشفيرُ (Encryption)،
البرمجياتُ الخبيثةُ (Malware)،
الهجماتُ التصيُّديةُ (Phishing Attacks)،
برمجياتُ الفديةِ (Ransomware)،
الثغراتُ الأمنيةُ (Security Vulnerabilities)،
الهجماتُ الموزَّعةُ لحجبِ الخدمةِ (DDoS Attacks)،
سرقةُ الهُويّةِ (Identity Theft)،
الهندسةُ الاجتماعيةُ (Social Engineering).

منتجات التعلّم
(Learning Products)

كُتيب رقمي يوضح تهديدات الأمن السيبراني لمشاركته خلال الحملة التوعوية لأفضل ممارسات الأمن السيبراني.

نتاجاتُ التعلُّمِ (Learning Outcomes)

- أبين أهداف الامن السيبراني.
- أوضحُ تهديداتِ الأمنِ السيبرانيِّ وحمايةِ البياناتِ الشخصيةِ.
- أشرحُ التنازلاتِ الناتجةَ عنِ اختيارِ توصياتِ الأمنِ السيبرانيِّ المختلفةِ وتنفيذِها.
- أبينُ مفهومَ الهجماتِ الإلكترونيةِ والاعتداءِ الإلكترونيِّ.
- أعدِّدُ أمثلةً على الوسائلِ الماديةِ والوسائلِ الرقميةِ للحمايةِ.
- أوضحُ كيفَ تقومُ وسائلُ الأمنِ الماديةُ والرقميةُ بحمايةِ المعلوماتِ.
- أناقشُ التكاملَ الوظيفيَّ بينَ الوسائلِ الماديةِ والرقميةِ لحمايةِ البياناتِ المتبادلةِ.
- أناقشُ قضايا واقعيةً تتعلقُ بالأمنِ السيبرانيِّ

تعرفتُ في الدرسِ السابقِ أمنَ المعلوماتِ وعلاقتَهُ بالأمنِ السيبرانيِّ. ولكنْ ما التهديداتُ المتعلقةُ بالأمنِ السيبرانيِّ؟ وما هيَ أفضلُ الطرقِ للتصدّي لها؟

نشاط تمهيدي

أذكرُ أحداثًا أمنيةً عالميةً أوْ عربيةً متعلقةً بالبياناتِ الرقميةِ منْ هجماتٍ، أوْ إتلافِ بياناتٍ، أوِ اختراقاتٍ، أوْ غيرِها شاهدتُها أوْ سمعتُ عنها، أوْ تعرضَ لها أحدُ معارفي. أناقشُ معَ الزملاءِ طبيعةَ الحدثِ وأثرَهُ في البياناتِ والأفرادِ والمؤسساتِ

الأمنُ السيبرانيُّ

في عامَيْ 2013 و2014 تعرضتْ شركةُ Yahoo، وهيَ شركةُ خدماتٍ حاسوبيةٍ أمريكيةٌ، لاثنينِ منْ أكبرِ اختراقاتِ البياناتِ في التاريخِ؛ حيثُ اختُرقتْ بياناتُ 3 مليارات حسابٍ في 2013 و500 مليونِ حسابٍ في 2014. وتضمنتِ البياناتُ المسروقةُ أسماءَ المستخدمينَ وكلماتِ المرورِ غيرِ المشفرةِ؛ مما أثرَ بشكلٍ كبيرٍ في سمعةِ الشركةِ، وأدى إلى خسائرَ ماليةٍ ضخمةٍ. هذا الحدثُ وغيرُهُ أظهرَ أهميةَ وجودِ أمنٍ سيبرانيٍّ، والحاجةَ المستمرةَ لتحسينِ التدابيرِ الأمنيةِ، وتبني أفضلِ الممارساتِ لحمايةِ البياناتِ الحساسةِ.

يتكون الأمنِ السـيبرانيِّ من طبقاتٍ متعددةٍ منَ الحمايةِ، تأتي على شكلِ مجموعةٍ منَ الممارساتِ والتقنياتِ والإجراءاتِ التي تهدفُ إلى حمايةِ الأنظمةِ والشبكاتِ والبياناتِ والبنيةِ التحتيةِ الرقميةِ منَ الهجماتِ والاعتداءاتِ الإلكترونيةِ. يهدفُ الأمنُ السيبرانيُّ إلى:

- **حمايةِ البياناتِ**: تأمينُ البياناتِ الحساسةِ والشخصيةِ منِ الوصولِ غيرِ المصرحِ بهِ أوْ السرقةِ.
- **سـلامةِ النظامِ**: ضمانُ أنَّ الأنظمةَ والبرامجَ تعملُ بشكلٍ صحيحٍ منْ دونِ تعرُّضِها للتلاعبِ أوِ الاختراقِ.
- **توافرِ الخدمةِ**: الحفاظُ على استمراريةِ الخدماتِ والتطبيقاتِ منَ الانقطاعِ أوِ التعطيلِ الناتجِ عنِ الهجماتِ.
- **الخصوصيةِ**: حمايةُ المعلوماتِ الشخصيةِ منِ الكشفِ أوِ الاستخدامِ غيرِ المصرحِ بهِ.
- اكتشافِ الهجماتِ والاستجابةِ لها.

نشاط

أزورُ الموقعَ الإلكترونيَّ للمركزِ الوطنيِّ للأمنِ السيبرانيِّ في الأردنِّ عبرَ الرابطِ :

(https://www.ncsc.jo) أوْ بمسحِ الرمزِ سريعِ الاستجابةِ المجاورِ.

أستكشفُ الموقعَ وأتعرفُ إلى الخدماتِ الرئيسةِ التي يقدمُها المركزُ، وأشاركُ الزملاءَ ما أتوصلُ إليهِ.

إثراء

المركزُ الوطنيُّ للأمنِ السـيبرانيِّ هوَ مؤسسـةٌ حكوميةٌ، تهدفُ إلى بناءِ منظومةٍ فعالةٍ للأمنِ السيبرانيِّ على المستوى الـوطنيِّ وتطويرِهـا وتنظيمِها؛ لحمايـةِ المملكـةِ مـنْ تهديداتِ الفضاءِ السيبرانيِّ ومواجهتِها بكفاءةٍ وفاعليـةٍ، بمـا يضمنُ استدامةَ العملِ، والحفاظَ على الأمنِ الوطنيِّ، وسلامةَ الأشخاصِ والممتلكاتِ والمعلوماتِ.

ولغاياتِ إيجادِ فضاءٍ سيبرانيٍّ أردنيٍّ آمنٍ وموثوقٍ، يسعى المركزُ إلى تدريبِ موظفي القطاعِ العامِّ والخاصِّ وجميعِ فئاتِ المجتمعِ، وتأهيلِهم وتوعيتِهم وتثقيفِهم، وإكسابِهم المعرفةَ والمهاراتِ اللازمةَ للحدِّ منَ المخاطرِ والتهديداتِ وفقًا لأفضلِ الممارسـاتِ في مجالِ الأمنِ السيبرانيِّ، وبما يضمنُ أعلى مسـتوىً منَ الكفاءةِ، وجعلِ الأردنِّ مركزَ إبداعٍ وتميزٍ إقليميٍّ ودوليٍّ في هذا المجالِ.

تهديداتُ الأمنِ السيبرانيِّ (Cyber Security Threats)

التهديداتُ المتعلقةُ بالأمنِ السيبرانيِّ هيَ محاولاتٌ أوْ إجراءاتٌ خبيثةٌ تهدفُ إلى إلحاقِ الضررِ بأنظمةِ المعلوماتِ، أوِ الشبكاتِ، أوِ البياناتِ الخاصةِ بالمؤسساتِ، أوِ الأفرادِ. هذهِ التهديداتُ يمكنُ أنْ تكونَ منْ مصادرَ داخليةٍ أوْ خارجيةٍ، منْ منظماتٍ أوْ أفرادٍ، وتهدفُ إلى التلاعبِ بالمعلوماتِ، وسرقتِها، أوْ إتلافِها.

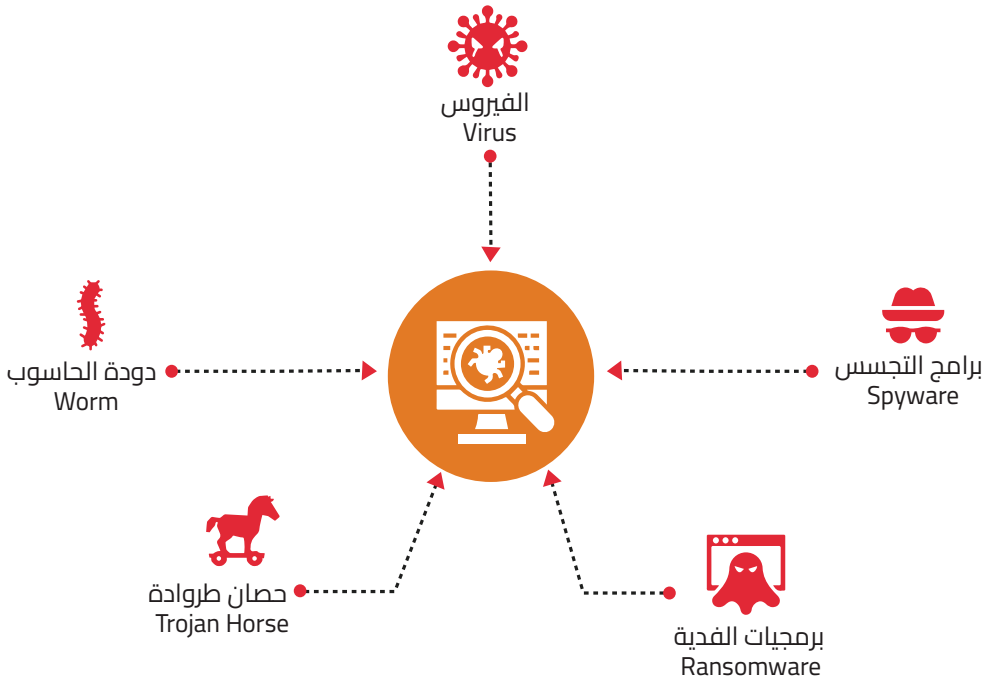
ومنْ بينِ أبرزِ مشكلاتِ الأمنِ السيبرانيِّ ما يأتي:

أولًا: البرمجياتُ الخبيثةُ (Malware)

وهيَ برامجُ ضارةٌ تصيبُ الأنظمةَ الحاسوبيةَ بهدفِ التدميرِ أوِ التجسسِ أوْ سرقةِ البياناتِ. ويمكنُ أنْ تؤديَ إلى فقدانِ البياناتِ، وتعطيلِ الأنظمةِ، وسرقةِ المعلوماتِ الحساسةِ،

كما هوَ موضحٌ في الشكلِ (2-1). ومنْ الأمثلةِ عليها:

- **الفيروساتُ (Viruses)**: تصيبُ الملفاتِ والبرامجَ، وتتكاثرُ عندَ تشغيلِ الملفِّ المصابِ.
- **ديدانُ الحاسوبِ (Worms)**: تنتشرُ عبرَ الشبكاتِ وتستغلُّ الثغراتِ الأمنيةَ منْ دونِ الحاجةِ إلى تفاعلِ المستخدمِ
- **برمجياتُ الفديةِ (Ransomware)**: تُقفلُ الأنظمةُ أوْ تشفرُ البياناتِ، وتطلبُ فديةً لإعادتِها.
- **برامجُ التجسسِ (Spyware)**: تراقبُ نشاطَ المستخدمِ وتسرقُ المعلوماتِ الحساسةَ منْ دونِ علمِهِ.



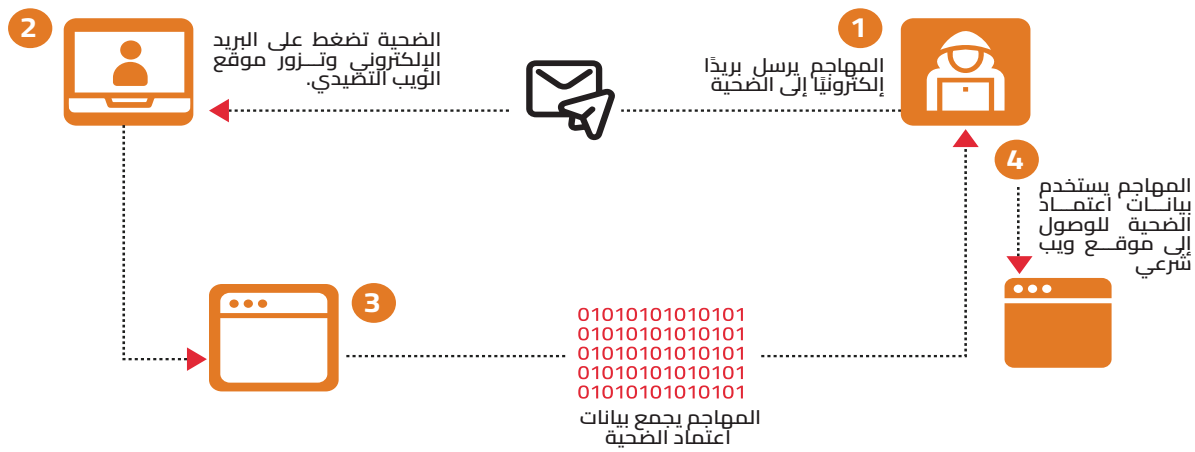
الشكل (2-1): بعضُ أنواعِ البرمجياتِ الخبيثةِ

نشاط جماعي

أبحثُ عبرَ المواقعِ الإلكترونيةِ الموثوقةِ لاختيارِ برنامجٍ خبيثٍ محددٍ، وجمعِ معلوماتٍ مفصلةٍ حولَهُ، تشملُ نوعَ البرنامجِ، وطرقَ انتشـــارِهِ، والتأثيراتِ السلبيةَ التي يحدثُها، وكيفيةَ الكشفِ عنهُ وإزالتِهِ، والإجراءاتِ الوقائيةَ الممكنـــةَ. أدونُ هذهِ المعلوماتِ في ملفٍّ (Google Docs)، وأشـــاركُهُ على اللوحِ التفاعليِّ الرقميِّ للصفِّ. بعدَ ذلكَ، نعرضُ نتائجَ بحثِنا في الصفِّ أمامَ الزملاءِ، ونقارنُ البرامجَ الخبيثةَ المختلفةَ استنادًا إلى المعاييرِ التي حدَّدْناها مسبقًا.

ثانيًا: التصيُّد الاحتياليُّ (Phishing)

محاولاتٌ احتياليةٌ للحصولِ على معلوماتٍ حساســـةٍ عنْ طريقِ تقمُّصِ هُويةِ جهاتٍ موثوقةٍ عبرَ البريدِ الإلكترونيِّ أوِ الرسائلِ النصيةِ أوِ المواقعِ المزيفةِ. ويمكنُ أنْ تؤديَ إلى سرقةِ الهُويةِ، وفقدانِ المعلوماتِ الماليةِ، والاختراقاتِ الأمنيةِ. انظرِ الشكلَ (2-2).



الشكل (2-2): عملية الهجوم بالتصيُّد الاحتيالي

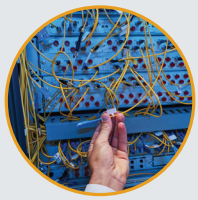
ثالثًا: الثغراتُ الأمنيةُ (Security Vulnerabilities)

الثغراتُ الأمنيةُ هيَ نقاطُ ضعفٍ أوْ عيوبٌ في الأنظمةِ أوِ البرامجِ أوِ الشـــبكاتِ، يمكنُ أنْ تُستغلَّ منْ قِبلِ المهاجمينَ لاختراقِ النظامِ والوصولِ إلى بياناتٍ حساسةٍ، أوِ القيامِ بتصرفاتٍ ضارةٍ. انظرِ الشكلَ (2-3) الذي يوضحُ أبرزَ أنواعِ الثغراتِ الأمنيةِ.

أبرزُ أنواعُ الثغراتِ الأمنيةِ، هيَ:

ثغرات البرمجيات
Software Vulnerabilities

تحـدث نتيجة وجود أخطـاء فـي كتابـة الكـود البرمجي، أو ثغرات فـي التعامل مع المدخـلات غير الموثوقة.



ثغرات الشبكة
Network Vulnerabilities

تشـمل نقاط ضعف في تكوينـات الشـبكة أو البروتوكـولات، مثـل ضعـف بروتوكـولات التشفير (SSL /TLS)، أو الشـبكات اللاسلكية غير المؤمنة.

ثغرات الإجراءات
Procedural Vulnerability

هـذه الثغـرات تتعلق بكيفية تنفيذ العمليات، ويمكـن أن تـؤدي إلى مخاطر أمـان، أو فقدان البيانـات، أو انتهـاك خصوصية، مثل ضعف إجـراءات التحقق من الهُويّـة، وعـدم وجود خطوات كافيـة لتأكيد هُويّة المستخدمين قبل منحهـم الوصـول إلى الأنظمة.

ثغرات الأجهزة
Hardware Vulnerabilities

تشـمل نقـاط ضعـف فـي المعـدات، مثـل معالجات الحواسـيب. وأحد أشـهر الأمثلة هي ثغرات "Meltdown" و "Spectre" التي أثرت في معالِجات شـركات عدة.

الشكلُ (2-3) أبرزُ أنواعِ الثغراتِ الأمنيةِ

أبحثُ

أبحث في المواقع الإلكترونية الموثوقة حول الثغرات الأمنية (Meltdown) و (Spectre). ثم أكتب تقريرًا باستخدام Google Docs وأشاركه مع الزملاء في الصف.

إثراء

تعدُّ ثغرةُ Heartbleed المكتشفةُ في 2014، إحدى أشهرِ الثغراتِ الأمنيةِ التي أثرتْ في مكتبةِ OpenSSL، وهيَ مجموعةٌ منِ الأدواتِ والبرمجياتِ مفتوحةِ المصدرِ، تُستخدمُ لتوفيرِ الأمانِ والتشفيرِ في الاتصالاتِ عبرَ الإنترنتْ؛ مما سمحَ للمهاجمينَ بسرقةِ معلوماتٍ حساسةٍ منِ الذاكرةِ. هذا الخللُ أبرزُ أهميةِ التحققِ الأمنيِّ المستمرِّ في البرمجياتِ المفتوحةِ المصدرِ.

نشاط جماعي

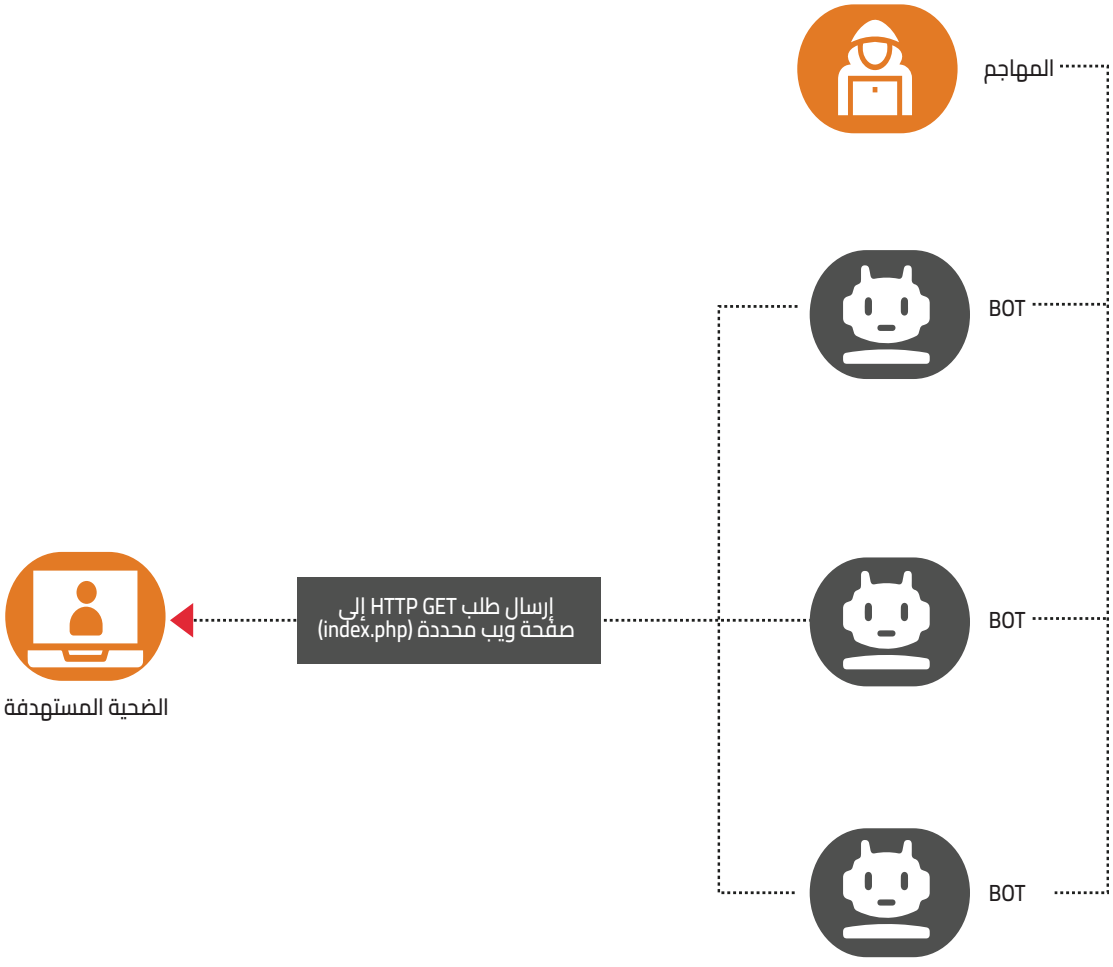
أفكرُ وأناقشُ

أفكرُ في إجراءاتٍ يمكنُ تطبيقُها ضمنَ نظامِ التشغيلِ المتوافرِ على الأجهزةِ؛ للحدِّ منَ الثغراتِ الأمنيةِ أوِ الوصولِ غيرِ المصرحِ بهِ، وأبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ، وأناقشُ زملائِي في المجموعةِ في ما توصلتُ إليهِ، وندونُ ما نتفقُ عليهِ منْ أفكارٍ استعدادًا لعرضِها ومناقشتِها معَ المجموعاتِ الأخرى في الصفِّ.

رابعًا: حجبُ الخدمةِ الموزَّعة (Distributed Denial of Service: DDoS)

هجومُ (DDoS) هوَ نوعٌ منْ هجماتِ(Denial of Service – Dos) يتمُّ فيهِ إغراقُ نظامٍ أوْ خادمٍ معينٍ بعددٍ هائلٍ منَ الطلباتِ بشـــكلٍ متزامنٍ منْ مصادرَ موزعةٍ عدةٍ؛ بهدفِ إيقافِ عملِ النظامِ أوْ جعلِهِ غيرَ قادرٍ على الاستجابةِ للمستخدمينَ الشرعيينَ.

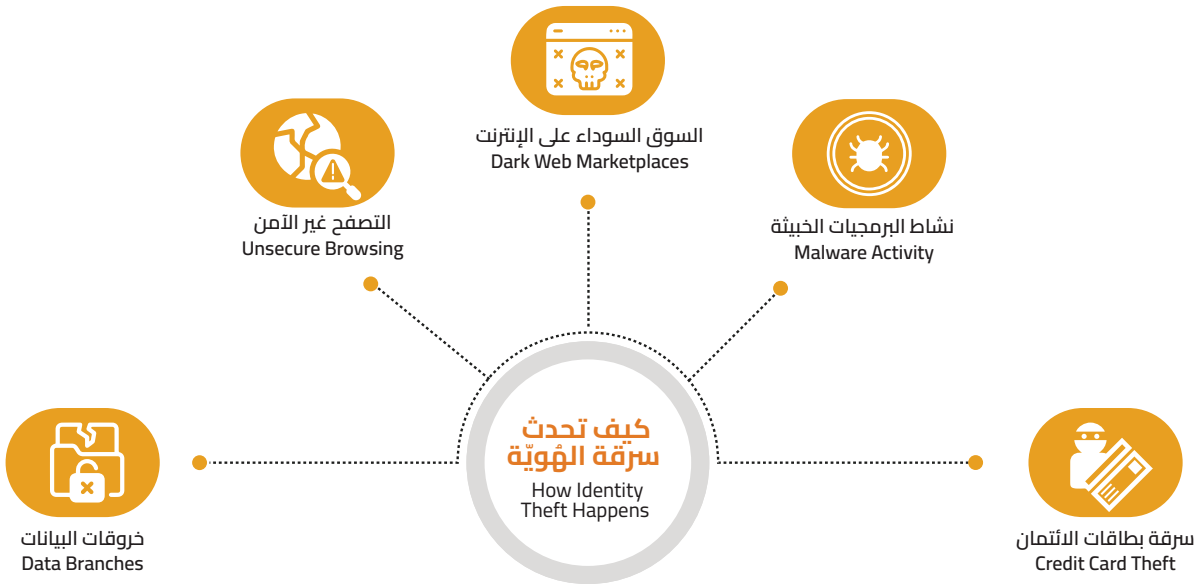
تنفَّذُ هجماتُ (DDoS) باســـتخدامِ شبكةٍ منَ الأجهزةِ المخترقةِ تُسمى (Botnet) ، ويتُحكمُ بها عنْ بعدٍ منْ قبلِ المهاجمينَ. وقدْ تكونُ هذهِ الهجماتُ على مستوى الشبكةِ أوْ على مستوى التطبيقِ أوْ على مســـتوى البياناتِ. انظر الشكلُ (2–4) الذي يوضحُ كيفيةَ استخدامِ مجموعةٍ منَ (Bots) منْ قبلِ المهاجمِ لشنِّ هجومٍ إلكترونيٍّ؛ حيثُ تكونُ مبرمجةً لإرسالِ طلبِ (HTTP GET) إلى صفحةِ ويب محددةٍ (index.php)؛ مما قدْ يؤدي إلى تعطيلِ خدماتِ الموقعِ الإلكترونيِّ المســـتهدفِ عنْ طريقِ إغراقِ النظامِ بطلباتٍ أكثرَ منْ التي يمكنُهُ التعاملُ معها. قدْ تواجهُ الضحيةُ المستهدفةُ في هذهِ الحالةِ تباطؤًا أوْ توقُّفًا كاملًا لخدماتِ الموقعِ بسببِ هذا الهجومِ.



الشكل (2–4): هجمات حجب الخدمة الموزعة

خامسًا: سَرقةُ الهُويّةِ (Identity Theft)

وتعني استخدامَ معلوماتٍ شخصيةٍ مسروقةٍ، مثلَ الاسمِ، وتاريخِ الميلادِ، ورقمِ الهويةِ أوِ الضمانِ الاجتماعيِّ، أوْ معلوماتٍ ماليةٍ، مثلَ أرقامِ الحساباتِ المصرفيةِ، وبطاقاتِ الائتمانِ لتمثيلِ شخصٍ آخرَ منْ دونِ إذنِهِ. ويمكنُ أنْ تؤديَ إلى خسائرَ ماليةٍ، وأضرارٍ بالسمعةِ، وتعقيداتٍ قانونيةٍ للضحيةِ. ويمكنُ أنْ تحدُثَ بطرقٍ مختلفةٍ. الشكلُ (2-5) يبينُ بعضَ طرقِ سرقةِ الهُويةِ.



الشكل (2-5): بعضُ طرقِ سرقةِ الهُويّةِ

نشاط جماعي

أتعاونُ معَ زملائِي في المجموعةِ على تصميمِ ملصقٍ باستخدامِ أحدِ برامجِ التصميمِ، يمثلُ بعضَ طرقِ سرقةِ الهُويةِ، معَ ذكرِ إجراءٍ في كلِّ حالةٍ يساعدُ على التقليلِ منَ الوقوعِ ضحيةً للسرقةِ، وأشاركُهُ على اللوحِ التفاعليِّ الرقميِّ للصفِّ. أتصفحُ ملصقاتِ زملائِي في المجموعاتِ الأخرى، وأناقشُهمْ في الطرقِ التي عرضوها والإجراءاتِ المقترحةِ لمواجهتِها.

سادسًا: الهندسةُ الاجتماعيةُ (Social Engineering)

هيَ تقنيةٌ احتياليةٌ تعتمدُ على التلاعبِ النفسيِّ بالأفرادِ لاستدراجِهم للكشفِ عنْ معلوماتٍ حساسةٍ، أوِ القيامِ بأفعالٍ معينةٍ تساعدُ المهاجمينَ على اختراقِ الأنظمةِ أوْ سرقةِ البياناتِ. وبدلًا منَ استخدامِ تقنياتِ الاختراقِ التقليديةِ المباشرةِ، يعتمدُ المهاجمونَ في الهندسةِ الاجتماعيةِ على استغلالِ الثقةِ والخداعِ والتلاعبِ في العواطفِ والسلوكاتِ البشريةِ.

يبينُ الشكلُ (2-6) مراحلَ الهجماتِ باستخدامِ الهندسةِ الاجتماعيةِ.

الشكل (2-6): إجراءاتُ الهندسةِ الاجتماعيةِ

أبحث

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنْ مشكلاتٍ أخرى منْ مشكلاتِ الأمنِ السيبرانيِّ، وأكتبُ فقرةً عنْ كلٍّ منها في ملفٍّ (Google Docs)، وأشاركُهُ معَ الزملاءِ، وأتأكدُ منْ ضبطِ صلاحياتِ الوصولِ بشكلٍ يسمحُ لهمْ بالقراءةِ أوِ التعليقِ فقطْ.

الفرقُ بينَ الهجومِ الإلكترونيِّ والاعتداءِ الإلكترونيِّ

إنَّ الهجوم الإلكتروني والاعتداءَ الإلكترونيَّ يشـــكلانِ تهديدًا متزايدًا للأمنِ الرقميِّ والسيبرانيِّ. ويتطلبُ التصدي لهما فهمَ الفرقِ بينَهما، والاستراتيجياتِ المناسبةَ لكلِّ حالةٍ منها.

ويتلخصُ الفرقُ بأنَّ الهجومَ الإلكترونيَّ يشـــملُ أيَّ محاولةٍ غيرِ مشروعةٍ للوصولِ إلى الأنظمةِ الرقميةِ أوْ تعطيلِها، بينما يكونُ الاعتداءُ الإلكترونيُّ أكثرَ تركيزًا على التســـببِ في ضررٍ مباشـــرٍ وفوريٍّ للضحيةِ بنيَّةٍ خبيثةٍ واضحةٍ. يمكـــنُ أنْ تكونَ الاعتداءاتُ الإلكترونيةُ جزءًا منَ الهجماتِ الإلكترونيةِ؛ لكنَّها تتميزُ بتركيزِها على الأضرارِ الشخصيةِ والمباشرةِ.

أتعاونُ معَ زملائِي في المجموعةِ على تحليلِ المشكلاتِ الآتيةِ وتصنيفِها إلى اعتداءٍ إلكترونيٍّ أوْ هجومٍ إلكترونيٍّ، معَ توضيحِ سببِ التصنيفِ:

المشكلةُ	تصنيفُ المشكلةِ	
	اعتداءٌ إلكترونيٌّ	هجومٌ إلكترونيٌّ
تلقّى أحمدُ رســـالةَ بريدٍ إلكترونيٌّ منْ شخصٍ مجهولٍ يدّعي أنَّهُ منَ البنكِ، وطلبَ منهُ إدخالَ بياناتِ حســـابِهِ البنكيِّ عبرَ رابطٍ في الرسالةِ. بعدَ إدخالِ بياناتِهِ، تعرضَ حسابُهُ للسرقةِ.		
أرسلتْ مجموعةٌ منَ الأشخاصِ رسائلَ تهديدٍ وإهانةً إلى سارةَ عبرَ وسائلِ التواصلِ الاجتماعيِّ بسببِ صورةٍ نشرتْها. تسببتْ الرسائلُ في إيذائِها نفسيًّا، وجعلتْها تشعرُ بالخوفِ والقلقِ.		
تمكَّنَ مهاجمٌ إلكتروني منَ اختراقِ شبكةِ الشركةِ التي يعملُ فيها خالدٌ، وسرقَ بياناتِ العملاءِ المهمةَ، واستخدمَها للحصولِ على فديةٍ ماليةٍ مقابلَ إرجاعِها.		
نشرتْ نورُ معلوماتٍ شـــخصيةٍ لصديقتِها على وسائلِ التواصلِ الاجتماعيِّ منْ دونِ إذنٍ منها؛ مما تســـببَ في إحراجِها وتعرضِها للمضايقاتِ منْ أشخاصٍ آخرينَ.		
تعرضتْ منصةٌ إلكترونيةٌ لهجومٍ إلكتروني عنْ طريقِ إرسالِ آلافِ الطلباتِ الزائفةِ في وقتٍ قصيرٍ؛ مما أدى إلى تعطُّلِ الموقعِ بالكاملِ ومنعِ المستخدمينَ منَ الوصولِ إليهِ.		

نشاط جماعي

وسائلُ الحمايةِ منْ تهديداتِ الأمنِ السيبرانيِّ

تتنوعُ وسائلُ الحمايةِ منْ تهديداتِ الأمنِ السيبرانيِّ بينَ الحمايةِ الماديةِ والحمايةِ الرقميةِ، وتؤدي كلٌّ منهما دورًا مهمًا في تأمينِ الأنظمةِ والبُنى التحتيةِ منَ التهديداتِ السيبرانيةِ.

لنوضح المقصود بكل نوع:

- **الحمايةُ الماديةُ (Physical Security):**

تهـــدفُ الحمايةُ الماديةُ إلى تأمينِ الأجهزةِ الماديةِ والمعداتِ التي تســـتخدمُ في تخزينِ البياناتِ ومعالجتِها، وتضمنُ حمايةَ البنيةِ التحتيةِ الماديةِ للأنظمةِ. تشملُ هذهِ الوسائلُ الإجراءاتِ التي تمنعُ الوصولَ غيرَ المصرحِ بهِ إلى الأماكنِ التي تحتوي على المعداتِ الإلكترونيةِ والبياناتِ الحساسةِ.

- **الحمايةُ الرَّقْميّةُ (Digital Security):**

الحمايةُ الرقميةُ هيَ الوســـائلُ المســـتخدمةُ لحمايةِ البياناتِ والأنظمةِ الإلكترونيةِ منَ الهجماتِ الإلكترونيةِ. وهيَ تتعلقُ بالحمايةِ التِّقْنيةِ التي تشـــملُ الدفاعَ ضدَّ الاختراقاتِ، والبرامجِ الضارةِ، وسرقةِ البياناتِ، وغيرِها منْ التهديداتِ التي تستهدفُ الأنظمةَ الرقميةَ.

وفي ما يأتي بعضُ الإجراءاتِ والوسائلِ المتعلقةِ بالحمايةِ الماديةِ والحمايةِ الرَّقْميّةِ:

الوسائل المادية Physical Security Measures		الوسائل الرّقْميّة Digital Security Measures	
	**ضوابط الوصول الفيزيائي (Physical Access Controls):** استخدام الأقفال والمفاتيح والأجهزة البيومترية (مثل بصمات الأصابع أو ماسحات الوجه) لتقييد الوصول إلى المرافق والمعدات الحساسة.		**التشفير (Encryption)**
	**المراقبة بالفيديو (Video Surveillance):** استخدام الكاميرات الأمنية لمراقبة المداخل والمناطق الحساسة.		**المصادقة متعددة العوامل (Multi–Factor Authentication – MFA)**
	**الحُراس الأمنيون (Security Guards):** توظيف حراس أمن لتأمين المرافق والتحقق من هُويات الزوار.		**جدران الحماية (Firewalls)**
	**الحماية من الكوارث الطبيعية (Disaster Protection):** تدابير لحماية المعدات والبنية التحتية من الكوارث، مثل الحرائق والزلازل والفيضانات.		**البرامج المضادة للفيروسات (Antivirus Software)**

أبحث

أبحث في المواقع الإلكترونية الموثوقة حول تدابير الحماية من الكوارث الطبيعية. ألخص ما اجده على شكل نقاط واشاركها مع الزملاء في الصف.

نشاط فردي

أفكرُ وأحلّلُ:

أصنفُ أدواتِ الحمايةِ الآتيةَ إلى ماديةٍ أوْ رقميةٍ:

إدارةَ الهُويةِ والوصولِ، التحديثاتِ الأمنيةَ، النسخَ الاحتياطيَّ للبياناتِ، موضحًا سببَ التصنيفِ. ثمّ أبحثُ عنْ أمثلةٍ أخرى، وأشارِكُ هذهِ الأفكارَ معَ زملائِي عبرَ اللوحِ الرقميِّ التفاعليِّ للصفِّ.

إثراء

تسهمُ تقنياتُ الذكاءِ الاصطناعيِّ والتعلُّمِ الآليِّ في تعزيزِ الأمنِ السيبرانيِّ عنْ طريقِ توفيرِ أدواتٍ متقدمةٍ لتحليلِ البياناتِ واكتشافِ التهديداتِ والتعاملِ معها. يعززُ هذا منَ القدرةِ على التنبؤِ بالتهديداتِ، والتفاعلِ بشكلٍ أسرعَ معَ التهديداتِ المحتملةِ؛ مما يوفرُ حمايةً أكثرَ فعاليةً ضدَّ المخاطرِ السيبرانيةِ المتزايدةِ.

نشاط جماعي

التفكيرُ في حمايةِ الأمنِ السيبرانيِّ:

بشكل فردي أفكرُ في الحالاتِ التي يجبُ فيها استخدامُ الحمايةِ الماديةِ للحمايةِ منَ التهديداتِ السيبرانيةِ، والحالاتِ التي تتطلبُ حمايةً رقميةً أوْ كليْهما. أتعاونُ معَ زملائِي في المجموعةِ لتبادلِ الأفكارِ حولَ "متى تكونُ الحمايةُ الماديةُ مثلَ أقفالِ الأبوابِ أوِ الكاميراتِ ضروريةً، ومتى تكونُ الحمايةُ الرقميةُ مثلَ كلماتِ المرورِ أوِ التشفيرِ هيَ الخيارُ الأفضلُ" بعدَ ذلكَ، نلخصُ أفكارَنا ونتائجَنا لعرضِها، ونناقشُها معَ المجموعاتِ الأخرى في الصفِّ، ونستمعُ إلى آرائِهمْ، ونحللُ التوصياتِ المختلفةَ.

التكاملُ الوظيفيُّ بينَ الوسائلِ الماديةِ والرَّقْميّةِ لحمايةِ البياناتِ

عزَّزَ التكاملُ بينَ الوسائلِ الماديةِ والرقميةِ منْ حمايةِ البياناتِ عنْ طريقِ إنشاءِ طبقاتٍ متعددةٍ منَ الأمانِ؛ حيثُ تعملُ الوسائلُ الماديةُ على تأمينِ الوصولِ الفيزيائيِّ إلى المعداتِ والبياناتِ، بينما توفرُ الوسائلُ الرقميةُ الحمايةَ اللازمةَ للبياناتِ نفسِها عنْ طريقِ التشفيرِ والمصادقةِ وإدارةِ الهُويةِ. هذا النهجُ الشاملُ، يقللُ منْ نقاطِ الضعفِ، ويضمنُ أمانًا متكاملًا للبياناتِ المتبادلةِ.

ويشملُ التكاملُ الوظيفيُّ بينَ الوسائلِ الماديةِ والرقميةِ لحمايةِ البياناتِ المتبادلةِ ما يأتي:

1. **الأمانُ الماديُّ**: ويتضمنُ اتخاذَ إجراءاتٍ نذكرُ منْها:
   - **الحمايةَ الماديةَ للأجهزةِ**: تشملُ هذهِ الحمايةُ استخدامَ وحدات تخزين، وأقفالَ الأمانِ، وأنظمةَ المراقبةِ لمنعِ الوصولِ غيرِ المصرحِ بهِ إلى الأجهزةِ التي تخزنُ البياناتِ.
   - **التخلصَ الآمنَ منَ البياناتِ**: التخلصُ منَ البياناتِ الحساسةِ بشكلٍ آمنٍ من الاجهزة لمنعِ استردادِها.
2. **الأمانُ الرَّقْميُّ**: ويتضمنُ اتخاذَ إجراءاتٍ نذكرُ منْها:
   - **التشفيرَ**: تشفيرُ البياناتِ في أثناءِ النقلِ والتخزينِ لمنعِ الوصولِ غيرِ المصرحِ بهِ.
   - **استخدامَ برامجِ الحمايةِ منَ الفيروساتِ وبرامجِ مكافحةِ الاختراقِ**: وذلكَ لحمايةِ الأجهزةِ منَ البرامجِ الضارةِ والهجماتِ الإلكترونيةِ.
   - **تفعيلَ جدرانِ الحمايةِ**: منعُ الوصولَ غيرَ المصرحِ بهِ إلى الشبكاتِ.
   - **التحديثاتِ الأمنيةَ**: تحديثُ البرامجِ بانتظامٍ لإصلاحِ الثغراتِ الأمنيةِ المعروفةِ.
3. **الممارساتُ الجيدةُ للأمانِ**: وتتضمنُ:
   - **كلماتِ المرورِ القويةَ**: استخدامُ كلماتِ مرورٍ قويةٍ وفريدةٍ لكلِّ حسابٍ.
   - **التوعيةَ الأمنيةَ**: تدريبُ الموظفينَ على التهديداتِ الأمنيةِ وممارساتِ الأمانِ الجيدةِ.
   - **النسخَ الاحتياطيَّ للبياناتِ**: عملُ نَسخٍ احتياطيٍّ منَ البياناتِ بانتظامٍ في حالِ فقدانِها أوْ تلفِها.
   - **خططَ الاستجابةِ للحوادثِ**: وجودُ خططٍ محددةٍ للتعاملِ معَ اختراقاتِ البياناتِ.

وللحصولِ على أفضلِ نتائـــجِ الحمايةِ يجبُ العملُ على دمجِ الحلولِ الماديةِ والرقميةِ، والتحليلِ المتقدمِ للبياناتِ، وإجراءِ التحديثاتِ باســـتمرارٍ، بالإضافةِ إلى توظيفِ تقنياتِ الذكاءِ الاصطناعيِّ وإنترنتْ الأشياءِ .

إضاءةٌ

تُبيِّنُ اتجاهاتُ الأمنِ السيبرانيِّ في النصفِ الأولِ من عامِ 2024 استخدامَ المزيدِ منْ أدواتِ الأمنِ السيبرانيِّ، والذكاءِ الاصطناعيِّ، والتعلمِ الآليِّ لاكتشافِ التهديداتِ، والاستجابةِ لها بشكلٍ أسرعَ منْ البشرِ؛ إذْ يمكنُ لهذهِ التقنياتِ تحليلُ الأنماطِ والتنبؤُ بالهجماتِ المحتملةِ؛ مما يجعلُها رصيدًا قيمًا في حمايةِ البياناتِ الحساسةِ. وقدْ بينتْ زيادةُ هجماتِ برامجِ الفديةِ، ونقاطُ الضعفِ في الأمانِ والمتعلقةِ بإنترنت الأشـــياءِ الحاجةَ المتزايدةَ لمتخصصي الأمنِ السيبرانيِّ المهرةِ؛ لأنَّ التهديداتِ الســـيبرانيةَ أصبحتْ أكثرَ تعقيدًا، والطلبُ على الخبيرينَ الذينَ يمكنُهمْ الحمايةُ منْ هذهِ التهديداتِ أعلى منْ أيِّ وقتٍ مضى.

أبحث

أبحثُ في المواقعِ الإلكترونيـــةِ الموثوقةِ عنْ إمكانيةِ تأثيرِ تقنياتِ الذكاءِ الاصطناعيِّ وتعلّمِ الآلةِ في ظهورِ تهديداتٍ أمنيةٍ جديدةٍ، وأكتبُ مقالةً منْ صفحةٍ واحدةٍ عنْ ذلكَ، وأشـــاركُها عبرَ اللوحِ الرقميِّ التفاعليِّ للصفِّ، وأقرأُ بعضًا منْ مشاركاتِ زملائِي، وأتفاعلُ معَ مشاركتينِ على الأقلِّ عبرَ إعطاءِ رأيِي في المقالةِ، وطرحِ أسئلةٍ ومناقشةِ النقاطِ المثارةِ.

إثراء

أستكشفُ الموقعَ الرسميَّ للمركزِ الوطنيِّ للأمنِ السيبرانيِّ عنْ طريقِ الرابطِ الآتي، أوْ عبرَ مسحِ الرمزِ سريعِ الاستجابةِ المجاورِ

الرابط: https://www.ncsc.jo/Default/Ar

ثمَّ أبحثُ عنْ خدمةِ روادِ السايبر، وأتعرفُ أهميَّتَها وطريقةَ الانضمامِ إليها.

- **الوعـــيُ بالحقوقِ والواجباتِ**: الوعيُ بالحقوقِ في الفضـــاءِ الرقميِّ، مثلَ الخصوصيةِ، وأمانِ المعلوماتِ، وحريةِ التعبيرِ، وإدراكِ الواجباتِ المرتبطةِ باســـتخدامِ التكنولوجيا، مثلَ احترامِ خصوصيةِ الآخرينَ وحقوقِهمْ.
- **الأمانُ والمسؤوليةُ**: اســـتخدامُ أدواتِ الأمانِ، مثلَ كلماتِ المرورِ القويةِ، والمصادقةِ متعددةِ العواملِ، وبرامجِ مكافحةِ الفيروســـاتِ، والإبلاغُ عنْ أيِّ سلوكٍ مشـــبوهٍ أوِ اختراقاتٍ أمنيةٍ للجهاتِ المعنيةِ.
- **التثقيفُ والتدريبُ المستمرُّ**: المشاركةُ في برامجَ تعليميةٍ حولَ الأمنِ السيبرانيِّ؛ لتعزيزِ المعرفةِ بالتهديداتِ الحاليةِ وطـــرقِ الحمايةِ، وتعزيزِ ثقافةِ تبادلِ المعلوماتِ عـــنْ كيفيةِ التعاملِ معَ التهديداتِ السيبرانيةِ بينَ الأفرادِ والمجتمعاتِ.
- **المسؤوليةُ الأخلاقيةُ**: التفاعلُ بشكلٍ إيجابيٍّ ومحترمٍ معَ الآخرينَ في الفضاءِ الرقميِّ، والتصدي للإساءةِ عبرَ الإنترنت، والإسهامُ في بيئةٍ رقميةٍ صحيةٍ.

مشروع

المشروعُ: حملةٌ إعلاميةٌ توعويةٌ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ/ مهمة 2

أتعاونُ معَ زملائِـــي لإنتاجِ المهمةِ الثانيةِ في الموادِّ التوعويةِ والتي تتمحورُ حولَ إنتاجِ كتيبٍ رقميٍّ، يوضحُ تهديداتِ الأمنِ السيبرانيِّ؛ لمشاركتِهِ في حملةٍ توعويةٍ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ.

يمكنُكَ اتباعُ الخطواتِ الآتيةِ،مراحلُ إنتاجِ الكُتيبِ الرَّقْميِّ:

1. **التخطيطُ:**

أحدّدُ الفصولَ والمحتوى الأساسيَّ مثلَ:

- **صفحةِ الغلافِ:** تتضمنُ العنوانَ " تهديداتُ الأمنِ السيبرانيِّ" وصورةً مناسبةً.
- صفحةٍ تخصُّ كلَّ تهديـــدٍ منَ التهديداتِ الواردةِ في الدرسِ، معَ شـــرحٍ مختصرٍ لها وصورةٍ مناسبةٍ.
- إضافةِ روابطَ لمواقعَ مفيدةٍ، مثلَ موقعِ المركزِ الوطنيِّ للأمنِ السيبرانيِّ.
- إضافةِ صفحةٍ نهائيةٍ، أكتبُ فيها ممارساتٍ تفيدُ في الحمايةِ منَ التهديداتِ.
- كتابةِ مسودةٍ أوليةٍ للمحتوى والتأكدَ منْ دقةِ المعلوماتِ.

2. **التصميمُ:**

- أستخدمُ برامجَ تصميمِ الكتيباتِ الرقميةِ مثلَ Canva أوْ Google Slides .
- أختارُ تصاميمَ جذابةً توضحُ التهديداتِ بشكلٍ بصريٍّ مميزٍ.
- أضيفُ صورًا توضيحيةً ورسومًا بيانيةً.
- أقسِّمَ المحتوى إلى أقسامٍ معَ عناوينَ فرعيةٍ واضحةٍ.

3. **المراجعة:**

- أتأكدُ منْ دقةِ المعلوماتِ، والتنظيمِ، وتناسقِ التصميمِ.
- أجري تعديلاتٍ لتحسينِ الوضوحِ والتصميمِ.

4. **النشـــرُ والمشاركةُ:** أحفظُ الكُتيبَ بصيغةِ PDF ، وأشاركُهُ عبرَ المنصاتِ الرَّقْميّةِ أوِ البريدِ الإلكترونيِّ.

أراعي عندَ عملِ الكُتيِّبِ:

- **الدقةَ والوضوحَ:** دقةُ المعلوماتِ المعروضةِ في الكتيبِ ووضوحُها.
- **التصميمَ:** تصميمٌ جذابٍ وتنسيقاتٌ جميلةٌ.
- استخدامَ صورٍ عاليةِ الدقةِ.
- الترتيبَ والتنظيمَ.
- دقةَ الروابطِ وفاعليَّتَها.

أقيِّم تعلُّمي

المعرفةُ: أوظفُ في هذا الدرسِ ما تعلمتُهُ منْ معارفَ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: ما أبرزُ تهديداتِ الأمنِ السيبرانيِّ؟ وكيفَ يمكنُ حمايةُ البياناتِ الشخصيةِ منها؟

.....

السؤالُ الثاني: أقارنُ بينَ الحمايةِ الماديةِ والحمايةِ الرقمية منْ حيثُ: الهدفُ، والوسائلُ، والأهميةُ.

.....

السؤالُ الثالثُ: أملأ الفراغَ بالمصطلحِ المناسبِ لكلِّ عبارةٍ في ما يأتي:

- ( ): الوسائل المستخدمة لحماية البيانات والأنظمة الإلكترونية من الهجمات الإلكترونية
- ( ): تقنية احتيالية تعتمد على التلاعب النفسي بالأفراد لاستدراجهم للكشف عن معلومات حساسة أو القيام بأفعال معينة تساعد المهاجمين على اختراق الأنظمة أو سرقة البيانات.
- ( ): نقاط ضعف في البرامج أو الأجهزة يمكن استغلالها للوصول غير المصرح به.
- ( ): برامج تراقب نشاط المستخدم وتسرق المعلومات الحساسة دون علمه

المهاراتُ: أستخدمُ مهاراتِ البحثِ الرقميِّ، والتفكيرَ الناقدَ والتواصلَ الرقميَّ، وأجيبُ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: أبحثُ عنْ وسائلَ أخرى لم تذكر في الدرس للحماية الماديةِ والرقميةِ المستخدمةِ في الأمانِ السيبرانيِّ وأذكرُ أمثلةً عليها.

السؤالُ الثاني: أفكرُ في قضايا واقعيةٍ تتعلقُ بالأمنِ السيبرانيِّ، وكيفيةِ التعاملِ معها بفعاليةٍ كأفرادٍ أوْ مؤسساتٍ.

السؤالُ الثالثُ: أبحثُ في أفكارٍ إبداعيةٍ يمكنُ تطبيقُها لزيادةِ أمنِ المعلوماتِ، والحمايةِ منَ التهديداتِ السيبرانيةِ.

القِيَمُ والاتجاهاتُ:

أتعاونُ معَ الزملاءِ لإطلاقِ مبادرةِ "روادِ السايبر" بحيثُ تتضمنُ المبادرةُ: تعريفَ الطلبةِ بخدمةِ روادِ السايبر التي أطلقَها المركزُ الوطنيُّ للأمنِ السيبرانيِّ، وطريقةِ الانضمامِ إليها، وعملِ نشاطٍ أسبوعيٍّ، يهدفُ إلى توعيةِ الطلبةِ وأولياءِ الأمورِ بالتهديداتِ السيبرانيةِ، مثلَ بوستراتٍ أوْ استباناتٍ أوْ برامجَ إذاعيةٍ أوْ منشوراتٍ.

الدرسُ الثالثُ

النقلُ الآمنُ للبيانات
(Secure Data Transfer)

الفكرةُ الرئيسةُ:

التعرفُ إلى أهميةِ المعلوماتِ المتوافرةِ على الشبكةِ وقيمتِها والحاجةِ إلى حمايتِها، وعلى أهميةِ الخبراتِ السابقةِ في إنشاءِ توصياتِ الأمنِ السيبرانيِّ، والبحثُ في العلاقةِ بينَ احتياجاتِ المستخدمِ وتوصياتِ الأمنِ السيبرانيِّ، وإلى الطرقِ المستخدمةِ برمجيًا لحمايةِ البياناتِ.

المفاهيمُ والمصطلحاتُ:

ميزةُ الوصولِ للخدمةِ (Accessibility)، قَفلُ البصمةِ (Touch ID)، قفلِ الوجهِ (Face ID)، برمجياتُ المسحِ (Wiping).

نتاجاتُ التعلُّمِ (Learning Outcomes)

- أصفُ أهميةَ المعلوماتِ المتوافرةِ على الشبكةِ وقيمتَها، والحاجةَ إلى حمايتِها.
- أصفُ أهميةَ الخبراتِ السابقةِ في إنشاءِ توصياتِ الأمنِ السيبرانيِّ.
- أصفُ العلاقةَ بينَ احتياجاتِ المستخدمِ وتعارضِها (في بعضِ الأحيانِ) معَ توصياتِ الأمنِ السيبرانيِّ.
- أدركُ العلاقةَ بينَ ميزةِ الوصولِ للخدمةِ Accessibility وتوصياتِ الأمنِ السيبرانيِّ.

منتجاتُ التعلُّمِ
(Learning Products)

تصميمُ عرضٍ تفاعليٍّ باستخدامِ برمجيةِ (Genially) بعنوانِ " رحلةٌ آمنةٌ لبياناتي" ، ضمنَ الحملةِ التوعويةِ لأفضلِ ممارساتِ الأمنِ السيبرانيِّ.

كلُّ تطورٍ في العالمِ الرقميِّ المتسارعِ ينتجُ عنهُ بعضُ التحدياتِ والمخاطرِ. ويعدُّ نقلُ البياناتِ عبرَ الشبكاتِ منْ أكثرِ المخاطرِ التي تهدِّدُ أمنَها. فكيفَ يمكنُ التعاملُ معَ هذا التهديدِ؟

نشاط تمهيدي

أتأملُ المواقفَ الآتيةَ، ثمَّ أجيبُ عنْ السؤالِ الذي يليها:

الموقفُ الأولُ: مسابقةٌ في الرياضياتِ على مستوى المملكةِ، الطلبُ منَ المعلمِ اختيارَ أعلى خمسةِ طلبةٍ تحصيلًا في مادةِ الرياضياتِ.

ما البياناتُ التي سيستخدمُها المعلمُ؟

الموقفُ الثاني: وصلتْ مجموعةٌ منَ المساعداتِ إلى منطقةٍ محددةٍ، ويريدُ المسؤولونَ توزيعَ هذهِ المساعداتِ بعدالةٍ.

ما البياناتُ اللازمُ الحصولُ عليها لتوزيعِها بعدالةٍ؟

الموقفُ الثالثُ: دخلَ مريضٌ إلى قسمِ الطوارئِ في مستشفىً، ويريدُ الطبيبُ تشخيصَ حالتِهِ.

ما البياناتُ التي يحتاجُها الطبيبُ لتشخيصِ حالتِهِ؟

أتخيلُ أنَّ البياناتِ المطلوبةَ للمواقفِ السابقةِ لمْ يتمَّ الحصولُ عليها في الوقتِ الصحيحِ، فما الذي سيحدثُ؟

إنَّ انعدامَ توافرِ البياناتِ سيولدُ حالةً منَ الفوضى وعدمِ الاتزانِ في اتخاذِ القراراتِ، فالطبيبُ لنْ يستطيعَ أنْ يشخصَ حالةَ المريضِ ويكتبَ العلاجَ المناسبَ إلا إذا حصلَ على البياناتِ اللازمةِ عنْ حالتِهِ، ولنْ يستطيعَ المسؤولونَ منْ دونِ توافرِ البياناتِ اللازمةِ توزيعَ المساعداتِ بشكلٍ عادلٍ لمنْ يحتاجُها؛ مما سيولدُ حالاتٍ منَ الغضبِ بينَ الناسِ لعدمِ وصولِ المساعداتِ لمستحقيها. ثمَّ إنَّ اختيارَ طلبةٍ بشكلٍ عشوائيٍّ لمسابقةِ الرياضياتِ، سيؤدي إلى فشلِ المسابقةِ؛ لعدمِ اعتمادِها على بياناتٍ محددةٍ في انتقاءِ الطلبةِ.

أهميةُ البياناتِ وحمايتُها

قبلَ ثورةِ الإنترنتْ، كانتْ تُقَيَّمُ الشركاتُ عنْ طريقِ ممتلكاتِها الماديةِ الملموسةِ، منْ أجهزةٍ وعمالٍ وموادَّ وما إلى ذلكَ، ولكنْ معَ ثورةِ الإنترنتْ في عصرِنا الحاليِّ، تستمدُّ عديدٌ منَ الشركاتِ الرائدةِ في العالمِ قيمتَها منْ ممتلكاتِها الافتراضيةِ وهيَ البياناتُ، فمثلًا شـــركاتُ التكنولوجيا المتقدمةُ، مثلُ شـــركاتِ وســـائلِ التواصلِ الاجتماعيِّ، ومحركاتِ البحثِ، والتجارةِ الإلكترونيةِ، والذكاءِ الاصطناعيِّ، والحوسبةِ السحابيةِ، كلُّها تعملُ على تحقيقِ أرباحِها الضخمةِ منْ ملكيتِها للبياناتِ. وتعدُّ البياناتُ ممتلكاتٍ متناميةً؛ حيثُ يُنتجُ العالمُ حواليْ 2,5 كوينتيليون بايت منْ البياناتِ يوميًا، وهذا الرقمُ يتزايدُ يوميًا معَ اتصالِ مزيدٍ منَ الأشخاصِ والأجهزةِ بشبكةِ الإنترنتْ.

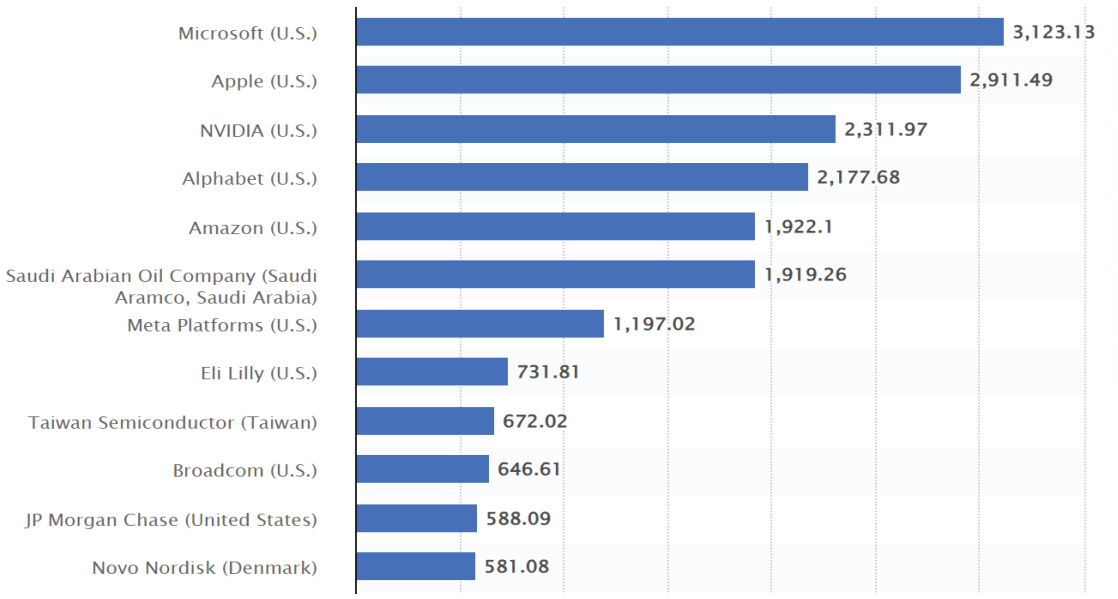
أبحثُ

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ على الإنترنت عنْ وحدةِ كوينتيليونَ. ما قيمتُها؟ وما ترتيبُها ضمنَ وحداتِ القياسِ؟ أشـــاركُ ما أتوصلُ إليهِ معَ الزملاءِ عنْ طريقِ اللوحِ الرقميِّ التفاعليِّ الخاصِّ بالصفِّ Padlet.

نلاحظُ منَ الشـــكلِ (3-1) الذي يمثلُ أكبرَ شـــركاتِ العالمِ من حيثُ القيمةُ السوقيةُ عامَ 2023 (المقدرة بمليار دولار أمريكي)، أنَّ أكبرَ شركاتٍ في العالمِ منْ حيثُ القيمةُ السوقيةُ هيَ شركاتُ بياناتٍ.

وهي كما يأتي:

- **شركةُ مايكروسوفت Microsoft**: وهيَ شركةُ تكنولوجيا عالميةٌ رائدةٌ في تطويرِ البرمجياتِ والخدماتِ الإلكترونيةِ والحلولِ.
- **شركةُ أبلْ**: شركةُ تكنولوجيا رائدةٌ في تطويرِ البرمجياتِ والخدماتِ الإلكترونيةِ والحلولِ حولَ العالمِ.
- **شركةُ نفيديا Nvidia**: وهيَ شركةٌ رائدةٌ بتصميمِ وحداتِ معالجةِ الرسومياتِ وتطويرِها (GPUs).
- **شركةُ ألفانتْ Alphanet**: وهيَ الشركةُ التي تملكُ موقعَ جوجل ويوتيوب.
- **شركةُ أمازون Amazon**: وهيَ شركةُ تكنولوجيا رائدةٌ في التجارةِ الإلكترونيةِ والحوسبةِ السحابيةِ والإعلاناتِ الافتراضيةِ.



الشكلُ (3-1): أكبرُ شركاتِ العالمِ منْ حيثُ القيمةُ السوقيةُ عامَ 2023

وتحققُ هذهِ الشركاتُ أرباحًا هائلةً عنْ طريقِ البياناتِ التي تملكُها. وأصبحتِ البياناتُ والمعلوماتُ المخزنةُ على الشبكةِ هيَ المادةُ الخامُ الجديدةُ للأعمالِ التجاريةِ، وهيَ مدخلاتٌ اقتصاديةٌ تكادُ تكونُ على قدمِ المساواةِ معَ رأسِ المالِ الماديِّ والعمالِ؛ حيثُ أصبحَ منَ الأسهلِ اليومَ، والأقلَّ تكلفةً على أيِّ شخصٍ جمعُ البياناتِ معَ ارتفاعِ قدراتِ الأجهزةِ الرقميةِ وانخفاضِ أسعارِها. وهذهِ البياناتُ لها تأثيرٌ في حياتِنا اليوميةِ، فعندما تنقرُ على إعجابٍ لإعلانٍ ما، أوْ عندما تملأُ معلوماتٍ في موقعٍ ما، فإنَّ ذلكَ يوفرُ للشركاتِ الرقميةِ بياناتٍ مهمةً، تساعدُها على التأثيرِ في قراراتِ العملاءِ والسلوكاتِ الشرائيةِ، ويعطي بياناتٍ للشركاتِ تساعدُها في تتبعِ هذهِ الحركاتِ، وبيعِ هذا السلوكِ للآخرينَ مقابلَ عائدٍ ماديٍّ.

إضاءةٌ

بلغتِ القيمةُ السوقيةُ للهُويةِ الرقميةِ للأشخاصِ في أوروبا؛ أيْ مجموعِ كلِّ المعلوماتِ المتاحةِ رقميًا عنْ الأشخاصِ "تريليون يورو".

أبحثُ

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنِ الهويةِ الرقميةِ في الأردنِّ وقيمتِها السوقيةِ، ثمَّ ألخصُ ما توصلتُ إليهِ منْ نتائجَ باستخدامِ ملفِّ (Google Docs)، وأشاركُهُ معَ الزملاءِ على اللوحِ التفاعليِّ الرقميِّ للصفِّ Padlet، وأناقشُ زملائِي في النتائجِ التي توصلنا إليها.

إضاءة

هناكَ عديدٌ منَ القوانينِ والتشريعاتِ التي تنظمُ حمايةَ البياناتِ، مثلَ اللائحةِ العامةِ لحمايةِ البياناتِ (GDPR) في الاتحادِ الأوروبيِّ، وقانونِ حمايةِ خصوصيةِ المستهلكِ في كاليفورنيا (CCPA). إنَّ عدمَ الامتثالِ لهذهِ القوانينِ يمكنُ أنْ يؤديَ إلى عقوباتٍ ماليةٍ كبيرةٍ وإجراءاتٍ قانونيةٍ صارمةٍ. في الأردنِّ، أصدرت الحكومةُ الأردنيةُ قانونَ حمايةِ البياناتِ الشخصيةِ في عامِ 2023 (يمكنُ الاطلاعُ عليهِ بمسحِ الرمزِ المجاورِ سريعِ الاستجابةِ).

أهميّةُ حمايةِ البياناتِ في الشبكةِ

يمارسُ الأفرادُ أنشطتَهمُ اليوميةَ باستخدامِ شبكاتِ الإنترنت، مثلَ العملِ، واللعبِ، والتسوقِ، ومشاهدةِ الأفلامِ، والتواصلِ معَ الآخرينَ، وطلبِ الطعامِ، ودفعِ الفواتيرِ، وغيرِها منَ الأنشطةِ اليوميةِ، ويتركُ ذلكَ مجموعةً كبيرةً منَ البياناتِ الخاصةِ بالأفرادِ مخزنةً في شبكةِ الإنترنت، ويمكنُ تتبعُ بياناتِ الأفرادِ بسهولةٍ عبرَ الشبكةِ؛ مما يتيحُ لمجرمي الإنترنتْ إلحاقَ الضررِ الكبيرِ عنْ طريقِ سرقةِ البياناتِ الحساسةِ والتلاعبِ بها. وتستغلُّ بعضُ الجهاتِ بياناتِ المستهلكينَ وسلوكاتِهمْ على مواقعِ التواصلِ، وتوجهُهمْ إلى مواقعِ تسويقٍ عدوانيةٍ أوْ متلاعبٍ بها، وترسلُ رسائلَ الإقناعِ المزعجةِ، وغيرِ المرغوبِ فيها.

لذا؛ يجبُ الالتزامُ بتوصياتِ الأمنِ السيبرانيِّ (Cybersecurity Recommendations) لحمايةِ هذهِ البياناتِ، وهيَ مجموعةٌ منِ المهاراتِ والعملياتِ التي صممتْ لحمايةِ الشبكةِ وأجهزةِ الحاسوبِ، والبرامجِ والبياناتِ منِ الهجماتِ، والوصولِ غيرِ المصرحِ بهِ للبياناتِ والبرامجِ الضارةِ.

نشاط فردي

أبحثُ وأناقشُ:

هلْ سمعتَ بمصطلحِ القرصنةِ الأخلاقيةِ (Ethical Hacking)؟ ابحثْ في المواقعِ الإلكترونيةِ الموثوقةِ عبرَ الإنترنت عنْ هذا المفهومِ، وعنْ كيفيةِ إسهامِ القرصنةِ الأخلاقيةِ في تعزيزِ أمنِ البياناتِ والشبكاتِ، والطرقِ التي يستخدمُها القراصنةُ الأخلاقيونَ لاختبارِ الأنظمةِ الأمنيةِ وتقويتِها. ألخصُ المعلوماتِ الرئيسةَ والنقاطَ التي توصلتُ إليها، وأشاركُها معَ زملائي في الصفِّ عنْ طريقِ مجموعةِ الصفِّ أوْ عبرَ البريدِ الإلكترونيِّ، وأناقشُ معهمْ أهميةَ القرصنةِ الأخلاقيةِ في الحفاظِ على أمنِ المعلوماتِ، وكيفَ يمكنُ أنْ تؤديَ دورًا فعالًا في الحدِّ منَ التهديداتِ السيبرانيةِ.

توصياتُ الأمنِ السيبرانيِّ

ظهورُ سياساتٍ وتوصياتٍ متعلقةٍ بالأمنِ السيبرانيِّ جاءَ كردٍّ فعلٍ للتطورِ السريعِ للتكنولوجيا، وزيادةِ استخدامِ الإنترنتْ في جميعِ جوانبِ الحياةِ. سنستعرضُ اثنينِ منْ أكبرِ هجماتِ الأمنِ السيبرانيِّ التي حصلتْ في التاريخِ، وكيفيةَ تأثيرِ هذهِ الهجماتِ في تشكيلِ توصياتِ الأمنِ السيبرانيِّ.

الهجومُ الأوَّلُ:

منْ أكبرِ الهجماتِ السيبرانيةِ في تاريخِنا المعاصرِ كانَ هجومُ (WannaCry) في عامِ 2017 الذي استهدفَ أنظمةَ التشغيلِ ويندوز (Windows)؛ حيثُ قامَ بتشفيرِ بياناتِ الضحايا ومطالبتِهمْ بمفتاحِ لفكِّ التشفيرِ، وقدْ أثرَ هذا الهجومُ في أكثرَ من 200000 حاسوبٍ في 150 دولةً، وكانَ هذا الهجومُ خطيرًا؛ لأنَّهُ استغلَّ ثغرةً أمنيةً في نظامِ التشغيلِ ويندوز، لمْ تكنْ معروفةً منْ قبلُ، ولمْ تكنْ كثيرٌ منِ المؤسساتِ مستعدةً لمثلِ هذا النوعِ منَ الهجومِ. كانَ الهجومُ سريعَ الانتشارِ، ومدمرًا؛ ولكنْ لحسنِ الحظِّ، اكتشفَ أحدُ الباحثينَ الأمنيينَ مفتاحَ التشفيرِ الذي أوقفَ انتشارَ البرامجِ الضارةِ، وقدْ ساعدَ هذا الهجومُ على سدِّ الثغرةِ الأمنيةِ الموجودةِ في نظامِ الويندوز، وركّزَ على ضرورةِ الانتباهِ إلى الثغراتِ الأمنيةِ في البرامجِ والتطبيقاتِ.

الهجومُ الثّاني:

هجومٌ اخترقَ بياناتِ شركةِ ائتمانٍ هيَ شركةُ إيكوفاكس (EQUIFAX)؛ بسببِ وجودِ ثغرةٍ أمنيةٍ في برنامجِ (Apache Struts)، وهوَ إطارُ عملٍ شائعٍ لتطبيقاتِ الويب، كانتْ إيكوفاكس تستخدمُهُ. فقدْ اخترقتِ السجلاتِ الخاصةَ لِ 147.9 مليونَ مواطنٍ أمريكيٍّ و15.2 مليونَ مواطنٍ بريطانيٍّ و19000 مواطنٍ كنديٍّ؛ مما جعلَها منْ أكبرِ الجرائمِ المتعلقةِ بسرقةِ الهويةِ، وتمكَّنَ المتسللونَ منَ الوصولِ إلى معلوماتٍ خاصةٍ وحساسةٍ، مثلَ أرقامِ الضمانِ الاجتماعيِّ، وتاريخِ الميلادِ، والعناوينِ؛ مما جعلَها منْ أكبرِ خروقاتِ البياناتِ في التاريخِ.

وانتقدَ عديدٌ منَ الأشخاصِ الشركةَ؛ بسببِ ممارساتِها الأمنيةِ السيئةِ؛ حيثُ تمكَّنَ المتسللونَ منَ الوصولِ إلى أنظمةِ الشركةِ عنْ طريقِ ثغرةٍ أمنيةٍ معروفةٍ، لمْ تصححْ، ولمْ تتَّخذِ الشركةُ خطواتٍ مناسبةً لحمايةِ بياناتِ عملائِها.

يتبينُ مما سبقَ أنَّ أبرزَ أسبابِ ظهورِ سياساتِ الأمنِ السيبرانيِّ وتوصياتِهِ هيَ:

1. **زيادةُ الهجماتِ السيبرانيةِ وتطورُها**: مثلُ التصيُّدِ الاحتياليِّ (Phishing)، والبرمجياتِ الخبيثةِ (Malware) ، وهجماتِ الفديةِ (Ransomware)..

2. **حمايةُ المعلوماتِ الحساسةِ والبياناتِ الشخصيةِ**: مثلُ تفاصيلِ البطاقاتِ المصرفيةِ، والسجلاتِ الطبيةِ وغيرِها.

3. **الامتثالُ للقوانينِ واللوائحِ**: وضعتِ الحكوماتُ والمنظماتُ لوائحَ، مثلَ اللائحةِ العامةِ لحمايةِ البياناتِ (GDPR) في الاتحادِ الأوروبيِّ، وقانونِ حمايةِ خصوصيةِ المستهلكِ في كاليفورنيا (CCPA) ؛ لإجبارِ الشركاتِ على حمايةِ بياناتِ المستخدمينَ وفرضِ عقوباتٍ على الاختراقاتِ.

4. **حمايةُ البنيةِ التحتيةِ الحيويةِ**: وتشملُ القطاعاتِ الحيويةِ، مثلَ قطاعِ الطاقةِ، والرعايةِ الصحيةِ، والنقلِ، والتعليمِ، وغيرِها.

5. **زيادةُ الاعتمادِ على العملِ عنْ بعدٍ والخدماتُ السحابيةُ**: معَ تبنّي المؤسساتِ لنماذجِ العملِ عنْ بعدٍ واستخدامِ الخدماتِ السحابيةِ، زادتِ الحاجةُ إلى سياساتِ الأمانِ السيبرانيِّ لحمايةِ البياناتِ المتنقلةِ.

ومنَ الأمثلةِ على سياساتِ الأمنِ السيبرانيِّ وتوصياتِهِ:

1. **سياسةُ كلماتِ المرورِ**: تتطلبُ هذهِ السياسةُ منَ الموظفينَ والأفرادِ إنشاءَ كلماتِ مرورٍ قويةٍ ومعقدةٍ، وتحديثَها بشكلٍ دوريٍّ، وعدمَ مشاركتِها معَ الآخرينَ.

2. **سياسةُ الوصولِ إلى الشبكةِ**: تحددُ هذهِ السياسةُ منْ يمكنُهُ الوصولُ إلى الشبكةِ الداخليةِ للمؤسسةِ، وكيفيةِ مراقبةِ هذا الوصولِ.

3. **سياسةُ استخدامِ البريدِ الإلكترونيِّ**: تهدفُ هذهِ السياسةُ إلى منعِ التصيدِ الاحتياليِّ والهجماتِ الإلكترونيةِ عنْ طريقِ توجيهِ الموظفينَ والأفرادِ إلى كيفيةِ التعاملِ معَ رسائلِ البريدِ الإلكترونيِّ المشبوهةِ.

4. **سياسةُ النسخِ الاحتياطيِّ واستعادةُ البياناتِ**: تضمنُ هذهِ السياسةُ وجودَ نُسخٍ احتياطيةٍ منْ البياناتِ الحيويةِ، وتحددُ إجراءاتِ استعادةِ البياناتِ في حالِ حدوثِ خرقٍ أمنيٍّ أوْ فقدانٍ للبياناتِ.

5. **سياسةُ التوعيةِ والتدريبِ**: تهدفُ إلى زيادةِ وعيِ الموظفينَ والمستخدمينَ بأفضلِ ممارساتِ الأمنِ السيبرانيِّ عنْ طريقِ التدريبِ المنتظمِ.

نشاط جماعي

أتعاونُ معَ زملائِي في المجموعةِ عنْ طريقِ البحثِ في المواقعِ الإلكترونيةِ الموثوقةِ على الإنترنتْ عنْ هجماتٍ سيبرانيةٍ خطيرةٍ، وأثرِها في توصياتِ الأمنِ السيبرانيِّ. ونعدُّ عرضًا تقديميًا باستخدامِ (Google Slides) عنْ واحدةٍ منْ تلكَ الهجماتِ، ونذكرُ تفاصيلَ الهجومِ، والطرقَ المستخدمةَ، والأضرارَ التي نجمتْ عنهُ، والدروسَ المستفادةَ، ونشاركُهُ على اللوحِ التفاعليِّ الرقميِّ للصفِّ، ونناقشُ الزملاءَ في المجموعاتِ الأخرى، ونجيبُ عنْ أسئلتِهِمْ واستفساراتِهِمْ حولَ الهجومِ وأثرِهِ، والتوصياتِ الأمنيةِ التي تبعتْهُ.

نشاط جماعي

أتعاونُ معَ الزملاءِ في الصفِّ لاقتراحِ إجراءاتٍ وطرقٍ لسياساتِ الأمنِ السيبرانيِّ، يمكنُ تطبيقُها على مستوى المدرسةِ، ثمَّ ندونُ الأفكارَ ونناقشُها، ونتبادلُ الآراءَ معَ المجموعاتِ الأخرى. وبعدَ الاتفاقِ على الإجراءاتِ والطرقِ، نعملُ معًا على تصميمِ بوستر باستخدامِ أحدِ برامجِ التصميمِ وننشرُهُ عبرَ الموقعِ الإلكترونيِّ للمدرسةِ، ضمنَ إطارِ حملةِ التوعيةِ بأفضلِ الممارساتِ للأمنِ السيبرانيِّ.

العلاقةُ بينَ احتياجاتِ المُستخدِمِ وتوصياتِ الأمنِ السيبرانيِّ

تنظرُ المؤسساتُ المختلفةُ إلى مسألةِ الخصوصيةِ وحمايةِ البياناتِ بشكلٍ مختلفٍ، فقدْ تهتمُّ بسرعةِ نقلَ البياناتِ أكثرَ منَ الاهتمامِ بخصوصيةِ البياناتِ وكذلكَ بالنسبةِ للأفرادِ. وقدْ تتعارضُ توصياتُ الأمنِ السيبرانيِّ في ما يتعلقُ بالحفاظِ على خصوصيةِ البياناتِ معَ رغباتِ الفردِ. ولتوضيحِ ذلكَ فلْنتأملِ الأمثلةَ الآتيةَ:

مثال (1):

أجرى باحثٌ في المجالِ الطبيِّ دراسةً على مرضى معينينَ منَ المجتمعِ، وأخذَ بياناتِ المرضى وحللَها، ونشرَ نتائجَ الدراسةِ. وبناءً على النتائجِ خصصتِ الحكومةُ الموارِدُ الماليةُ اللازمةُ لمعالجةِ المرضِ بناءً على بياناتِ المرضى التي نُشرتْ، واستفادَ الأطباءُ الآخرونَ منْ هذهِ البياناتِ لإجراءِ مزيدٍ منَ الدراساتِ. واستفادتْ شركاتُ التأمينِ الصحيِّ منَ البياناتِ. ولكنْ منَ الناحيةِ الأخلاقيةِ، تسببَ نشرُ بياناتِ الأفرادِ الخاصةِ بفقدانِ بعضِ الأفرادِ وظائفَهمْ وتشويهِ سمعتِهمْ.

مثال (2):

في أثناءِ جائحةِ كورونا، استخدمتْ عديدٌ منَ الدولِ خاصيةَ تتبُّعِ الأفرادِ المصابينَ ومراقبةِ تحركاتِهمْ عبرَ هواتفِهمْ؛ للحدِّ منْ انتشارِ المرضِ، علمًا بأنَّ بعضَ البلدانِ عارضتْ هذا الشأنَ بناءً على معيارٍ أخلاقيٍّ وهوَ انتهاكُ خصوصيةِ الأفرادِ.

مثال (3):

يدرسُ بعضُ الباحثينَ إمكانيةَ استخدامِ وسائلِ التواصلِ الاجتماعيِّ، وبياناتِ الأجهزةِ المحمولةِ لتحديدِ الأفرادِ المعرضينَ لخطرِ الانتحارِ، معَ أنَّ ذلكَ قدْ ينتهكُ خصوصيةَ الأفرادِ.

عندَ التأملِ في الأمثلةِ السابقةِ، نلاحظُ أنَّ الحاجةَ -في كثيرٍ منْ الأحيانِ- إلى مشاركةِ البياناتِ معَ الآخرينَ، قدْ تتعارضُ معَ توصياتِ الأمنِ السيبرانيِّ واختراقِ خصوصيةِ الفردِ، ويبقى الموضوعُ مرتبطًا بالغايةِ منْ مشاركةِ البياناتِ، فهلْ هيَ لصالحِ الخيرِ ومعالجةِ الأمراضِ وإنقاذِ الأرواحِ، أمْ أنَّ مشاركتَها لنْ تعودَ بالنفعِ على أحدٍ.

نشاط فردي

أُحللُ وأناقُش:

بعدَ أنْ درستُ بعضَ توصياتِ الأمنِ السيبرانيِّ لحمايةِ البياناتِ عبرَ شبكةِ الإنترنت، هلْ أعتقدُ أنَّ هذهِ التوصياتِ تتعارضُ معَ احتياجاتِي عندَ استخدامِ شبكةِ الإنترنت؟ أذكرُ بعضَ المواقفِ التي واجهتْني عندَ استخدامِ شبكةِ الإنترنتْ على هاتفِي أوْ على جهازِ الحاسوبِ الخاصِّ بي، والتي اضطررتُ فيها إلى عدمِ تطبيقِ إحدى توصياتِ الأمنِ السيبرانيِّ. أشاركُ هذهِ المواقفَ معَ الزملاءِ، معَ تبريرِ موقفِي، وأستمعُ لآرائِهمْ.

العلاقةُ بينَ ميزةِ الوصولِ للخدمةِ (Accessibility) وتوصياتِ الأمنِ السيبرانيِّ

تُعرَّفُ ميزةَ الوصولِ للخدمةِ (Accessibility) بأنَّها قدرةُ الجميعِ على استخدامِ منتجٍ أوْ خدمةٍ، أوْ إتاحةِ الوصولِ للجميعِ، بمنْ فيهمْ كبارِ السنِّ وذوي الإعاقةِ؛ عبرَ مجموعةٍ منَ القواعدِ والأنظمةِ.

الشكل (3-2): ميزةُ الوصولِ

ومنْ أهمِّ مشكلاتِ إمكانيةِ الوصولِ ما يأتي:

- بصريةٌ (كضعفِ البصرِ وعمى الألوانِ).
- حركيةٌ (كالأشخاصِ الذينَ يعانونَ منْ مشكلاتٍ في بعضِ الأطرافِ).
- سمعيةٌ (كفقدانِ السمعِ أوْ ضعفِهِ).
- إدراكيةٌ وتعلميةٌ (كمشكلاتِ عسرِ القراءةِ).
- عصبيةٌ (كمشكلاتِ الحساسيةِ للضوءِ).

وما يزالُ العالمُ الرَّقْميُّ بعيدٌ عنْ ميزةِ الوصولِ للخدمةِ بنسبةِ 100٪ للجميعِ، وما يزالُ عديدٌ منَ الأشخاصِ ذوي الإعاقاتِ المختلفةِ لا يستطيعونَ الوصولَ إلى كثيرٍ منَ المواقعِ أوِ الخدماتِ عبرَ شبكةِ الإنترنت، ويضطرونَ إلى الاعتمادِ على شخصٍ آخرَ في إنجازِ ذلكَ؛ وبهذا يكونونَ أكثرَ عرضةً لأخطارِ الأمنِ الرقميِّ وسرقةِ البياناتِ والهُويةِ..

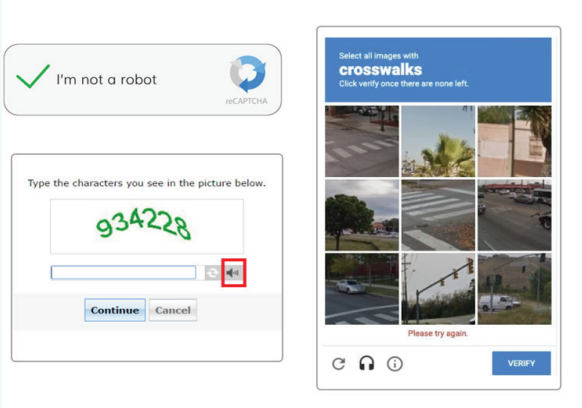
فعلى سبيلِ المثالِ، يجدُ الأشـــخاصَ الذينَ لديْهمْ إعاقةٌ بصريةٌ صعوبةً في استخدامِ الأجهزةِ أوِ التكنولوجيا التي لا تحتوي على ميزاتِ إمكانيةِ الوصولِ، مثلَ برامجِ قراءةِ الشاشةِ أوْ ميزةِ تكبيرِ الخطِّ، وقدْ يستعينونَ بأشخاصٍ آخرينَ، ويتعرضونَ بذلكَ إلى انتهاكِ خصوصيةِ بياناتِهمْ.

ويســـتخدمُ كثيرونَ أيضًا ميزةَ قفلِ البصمـــةِ (Touch ID) لحمايةِ أجهزتِهمُ الخلويةُ، ولكنَّ الأشـــخاصَ فاقدي الأطرافِ لا يستطيعونَ استخدامَ هذهِ الميزةِ.

وهناكَ أيضًا ميزةُ التعرفِ إلى الأشـــخاصِ عنْ طريقِ تقنيةِ قفلِ الوجهِ (Face ID) لفتحِ الأجهزةِ الخلويةِ. وقدْ يواجهُ الأشخاصُ منْ ذوي الإعاقةِ البصريةِ مشكلاتِ إمكانيةِ الوصولِ الى أجهزتِهم التكنولوجيةِ، إذا لمْ يقوموا بتحميلِ صورِهـــمْ بالاتجاهِ الصحيحِ في مواجهةِ الكاميرا بســـببِ عدمِ تمكُّنِهمْ منَ الرؤيةِ.

نشاط

أتأملُ الصورَ في الشكلِ (3-3) المجاورِ، هلْ واجهتُ هذهِ الصورةُ منْ قبلُ؟ ابحثْ عنْ ســـببِ ظهورِها في بعضِ المواقعِ؟ وعنْ علاقتِها بالأمنِ السيبرانيِّ. ماذا يعني الاختصارُ (CAPTCHA)؟ هلْ يســـتطيعُ جميـــعُ الأفرادِ التعاملَ مـــعَ هذهِ الصورِ بمنْ فيهمْ مـــنْ ذوي الإعاقاتِ المختلفةِ؟ أدونُ أفكاري وأشـــاركُها مـــعَ الزملاءِ.



الشكل (3-3): خياراتُ الوصولِ

لضمان حصول الجميع ومنهم ذوو الإعاقة على فرص متساوية للوصول إلى التطبيقات والتِقْنيّات عبر شـــبكة الإنترنت، والأدوات الرَّقْميّة التي تؤثر في سير حياتهم وتُسهِّلُها، وتحمي بياناتهم من الاختراق، ظهرتْ عديد من ميزات إمكانيةِ الوصول للخدمة التي يمكن أن تساعدهم، والتي تتوافق مع توصيات الأمن السيبراني.

نبيّن بعضها في ما يأتي:

- **قارئُ الشاشةِ (Screen Reader)**: يحولُ العناصرَ المرئيةَ على الشاشةِ مثلَ النصوصِ والأزرارِ والصورِ إلى كلامٍ أوْ لطريقةِ برايل (Braille)؛ مما يساعدُ الأشخاصَ ذوي الإعاقةِ البصريةِ على الوصولِ إلى المعلوماتِ بسهولةٍ.

- **الترجمـــةُ النصيةُ الفوريةُ**: نصـــوصٌ تظهرُ على الشاشـــةِ، تصفُ الـــكلامَ والأصواتَ في الفيديوهـــاتِ والبرامـــجِ التلفزيونيةِ؛ مما يســـاعدُ الأشـــخاصَ الصمَّ وضعافَ الســـمعِ.

- **التعـــرفُ الصوتيُّ**: ميزةٌ تســـمحُ للأشـــخاصِ باســـتخدامِ الأوامـــرِ الصوتيـــةِ للتحكمِ في الأجهـــزةِ؛ مما يفيـــدُ الأشـــخاصَ الذينَ يعانـــونَ صعوبـــةً في اســـتخدامِ الأيدي.

- **تصميـــمُ المواقعِ المتوافقةِ**: تصميمُ مواقـــعِ الويب؛ بحيثُ تكونُ قابلةً للاســـتخدامِ منْ قبلِ الأشخاصِ ذوي الاحتياجاتِ الخاصةِ، مثلَ اســـتخدامِ نصوصٍ بديلةٍ للصورِ، وتوفيرِ وسائطَ يمكنُ الوصولُ إليها بسهولةٍ وفقًا لاحتياجاتِهمْ

أبحثُ

أبحثُ في المواقعِ الإلكترونيةِ الموثوقـــةِ عبرَ الإنترنتْ عنْ ميزاتٍ أخرى لإمكانيةِ الوصولِ للخدمةِ، وأشاركُها معَ زملائِي في الصفِّ على اللوحِ الرقميِّ التفاعليِّ للصفِّ (Padlet).

نشاط عملي

محاكاةُ إدارةِ كلمةِ المرورِ:

أنشئُ معَ مجموعتي كلمةَ مرورٍ لملفٍّ المجموعةِ وفقَ المعاييرِ الآتيةِ:

- طولُ كلمةِ المرورِ 10.
- تحتوي على حرفٍ كبيرٍ على الأقلِّ.
- تحتوي على أرقامٍ ورموزٍ.

أختارُ مجموعةً أخرى، وأطلبُ إليها محاولةَ اكتشافِ كلمةِ المرورِ بعدَ طرحِ ثلاثةِ أسئلةٍ على مجموعتِنا في مدةِ (خمسِ دقائقَ).

إذا اكتشفتِ المجموعةُ كلمةَ المرورِ، يجبُ التفكيرُ في سببِ اكتشافِها، والبحثُ عنْ طريقةٍ لتحسينِ إنشاءِ كلمةِ المرورِ الخاصةِ بنا.

نشاط

أستخدمُ برمجيةَ سكراتش لإعدادِ برنامجٍ لتشفيرِ رسالةٍ مدخلةٍ باتباعِ طريقةٍ خاصةٍ بي (مثلَ تبديلِ الحروفِ؛ فالأولُ يصبحُ الأخيرَ، والثاني قبلَ الأخيرِ وهكذا)، ثمَّ أطبقَ البرنامجَ وأنفذُهُ؛ للتأكدِ منْ صحتِهِ. أشاركُ البرنامجَ معَ الزملاءِ، ونتشاركُ معًا فكَّ تشفيرِ الرسائلِ.

المُواطَنةُ الرَّقْميّةُ

- **حمايةُ المعلوماتِ الشخصيةِ**: تجنبُ مشاركةِ المعلوماتِ الشخصيةِ مثلَ العنوانِ، ورقمِ الهاتفِ، والمعلوماتِ الماليةِ على الإنترنت أوْ في المنتدياتِ العامةِ. واستخدامُ إعداداتِ الخصوصيةِ على منصاتِ التواصلِ الاجتماعيِّ؛ للحدِّ منْ وصولِ الغرباءِ إلى بياناتي.
- **احترامُ حقوقِ الملكيةِ الفكريةِ**: عدمُ تنزيلِ أوِ استخدامِ محتوىً غيرِ مرخصٍ، أوْ محميٍّ بحقوقِ الطبعِ والنشرِ منْ دونِ إذنٍ. واستخدامُ البرامجِ والتطبيقاتِ منْ مصادرَ شرعيةٍ ومتاجرَ رسميةٍ.
- **الوعيُ بالمخاطرِ الرقميةِ**: التعرفُ إلى هجماتِ التصيدِ الاحتياليِّ، وتجنبِ فتحِ الروابطِ المشبوهةِ، أوْ تحميلِ المرفقاتِ منْ مصادرَ غيرِ موثوقةٍ. وتحديثُ المعرفةِ حولَ أحدثِ تهديداتِ الأمنِ السيبرانيِّ، وكيفيةِ التعاملِ معها.
- **التفاعلُ المسؤولُ عبرَ الإنترنت**: تجنبُ نشرِ أوْ مشاركةِ معلوماتٍ زائفةٍ أوْ مضللةٍ، والإبلاغُ عنْ السلوكاتِ غيرِ القانونيةِ أوِ الضارةِ عبرَ الإنترنت مثلَ التنمُّرِ الإلكترونيِّ.
- **تحديثُ الأجهزةِ والبرمجياتِ بانتظامٍ**: التأكدُ منْ تحديثِ أنظمةِ التشغيلِ، وبرامجِ مكافحةِ الفيروساتِ، والتطبيقاتِ لضمانِ الحمايةِ ضدَّ الثغراتِ الأمنيةِ.

المشروعُ: حملةٌ إعلاميةٌ توعويةٌ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ/ مهمة 3

أتعاونُ معَ زملائِي لإنتاجِ المهمةِ الثالثةِ في الموادِّ التوعويةِ التي تتمحورُ حولَ تصميمِ عرضٍ تفاعليٍّ باستخدامِ برمجيةِ (Genially) بعنوانِ " رحلةٌ آمنةٌ لبياناتِي" ، لمشاركتِهِ في حملةٍ توعويةٍ عنْ أفضلِ ممارساتِ الأمنِ السيبرانيِّ.

باتباعِ الخطواتِ الآتيةِ:

- أنشئُ مقطعَ فيديو قصيرًا، يوضحُ كيفَ يمكنُ للبياناتِ أنْ تتعرضَ للاختراقِ. اشرحُ ذلكَ بذكرِ الأسبابِ، مثلَ كلماتِ المرورِ الضعيفةِ، واستخدامِ شبكاتٍ غيرِ آمنةٍ، وغيابِ التشفيرِ.
- أصممُ نموذجًا يحتوي على أزرارٍ تفاعليةٍ وعناصرَ قابلةٍ للنقرِ، توضحُ أفضلَ ممارساتِ الأمنِ السيبرانيِّ، مثلَ استخدامِ كلماتِ مرورٍ قويةٍ، وتفعيلِ التحققِ بخطوتينِ، وتجنبِ الشبكاتِ العامةِ، وتحديثِ البرامجِ بانتظامٍ.
- أقدمُ روابطَ ومصادرَ تتعلقُ بميزةِ الوصولِ للخدمةِ، والطرقِ المستخدمةِ برمجيًا لحمايةِ البياناتِ.
- أقدمُ روابطَ لمصادرَ ومقالاتٍ تتعلقُ بأفضلِ ممارساتِ حمايةِ البياناتِ، مثلَ تشفيرِ البياناتِ وبرمجياتِ الحمايةِ. وأتأكدُ منْ صحةِ الروابطِ، ومنْ تحديثِها.
- أنشئُ شريحةً تلخصُ النقاطَ الأساسيةَ لتوصياتِ الأمنِ السيبرانيِّ، مثلَ أهميةِ تشفيرِ البياناتِ، ومراقبةِ النشاطاتِ المشبوهةِ، والتعاملِ بحذرٍ معَ الروابطِ والملفاتِ.

أراعي عندَ تصميمِ العرضِ التفاعليِّ:

- **الشموليةَ والدقةَ:** المعلوماتُ في العرضِ دقيقةٌ خاليةٌ منَ الأخطاءِ وتغطّي المطلوبَ.
- التصميمَ المشوقَ والجذابَ، واستخدامَ المؤثراتِ البصريةِ والسمعيةِ.
- **دقةَ الروابطِ:** التأكدُ منْ صحةِ الروابطِ في العرضِ وفاعليتِها.
- السهولةَ في التعاملِ معَ العرضِ.

مشروع

أقيّمُ تعلُّمي:

المعرفةُ: أستخدمُ ما تعلمتُهُ منْ معارفَ في هذا الدرسِ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: ماذا تعني كلٌّ منَ المصطلحاتِ الآتيةِ:

المصطلح	المعنى
Accessibility	
Wiping	
Touch ID	
Face ID	

السؤالُ الثاني: أوضحُ أهميةَ الحاجةِ إلى حمايةِ المعلوماتِ على الشبكةِ، وأبررُ ذلكَ..

.....

السؤالُ الثالثُ: أعللُ ما يأتي:

أ. تستمدُّ العديدَ منَ الشركاتِ الرائدةِ في العالمِ قيمتَها منْ ممتلكاتِها الافتراضيةِ وهيَ البياناتُ.

.....

ب. حذفُ البياناتِ على القرصِ الصلبِ لنْ تكونَ خطوةً آمنةً.

.....

ج. ما يزالُ العالمُ الرقميُّ بعيدًا كلَّ البعدِ عنْ ميزةِ الوصولِ للخدمةِ بنسبةِ 100٪ للجميعِ.

.....

المهاراتُ: أستخدمُ مهاراتِ البحثِ الرَّقْميِّ، والتواصلَ الرَّقْميَّ، والتفكيرَ الناقدِ في الإجابةِ عنِ السؤالينِ الآتيينِ:

السؤالُ الأولُ: أفكرُ: كيفَ يمكنُ للأفرادِ معرفةُ التطوراتِ المتعلقةِ بالأمنِ السيبرانيِّ وتوصياتِهِ، وطرقِ اتباعِ الإجراءاتِ الصحيحةِ في التعاملِ معَ البياناتِ. أقدمُ مقترحاتٍ

السؤالُ الثاني: أبحثُ في تشريعاتٍ تخصُّ الأردنَّ وتتعلقُ بتوصياتِ الأمنِ السيبرانيِّ، وألخصُها في ملفِّ معالجِ النصوصِ، معَ وجودِ رابطٍ لكلٍّ منها يسهِّلُ الوصولَ إليها.

القِيَمُ والاتجاهاتُ:

بالتعاونِ معَ أفرادِ مجموعتي وباستخدامِ مواقعَ آمنةٍ في شبكةِ الإنترنت، أنشئُ بوسترًا باستخدامِ برمجيةٍ متاحةٍ، يحتوي على قائمةٍ بالبرمجياتِ والميزاتِ المتوافرةِ؛ لمساعدةِ ذوي الإعاقةِ على الوصولِ إلى التطبيقاتِ والمواقعِ، وأصنفُها بحسبِ نوعِ الإعاقةِ، ثمَّ أنشرُها على مواقعِ التواصلِ الاجتماعيِّ؛ ليستفيدَ منها كلُّ منْ يحتاجُها.

الدرسُ الرابعُ:

وسائلُ حمايةِ البياناتِ
(Data Protection Means)

منتجاتُ التعلُّمِ
(Learning Products)

خريطة ذهنية تفاعلية (Interactive Mindmap) عن وسائل حماية البيانات باستخدام أداة (Coggle).

الفكرةُ الرئيسةُ:

التعرفُ إلى وسائلِ الحمايةِ التي تحدُّ منْ مشكلاتِ مشاركةِ البياناتِ، وتقييمِ وسائلِ الحمايةِ منْ حيثُ فعاليتُها والجدوى منْ استخدامِها، وبيانُ العلاقةِ بينَ فعاليةِ وسائلِ الحمايةِ، وجدواها، وتأثيرِها الأخلاقيِّ.

المفاهيمُ والمصطلحاتُ:

تشفيرُ البياناتِ (Encryption)،
النسخُ الاحتياطيُّ (Backup and Recovery)،
ضبطُ صلاحياتِ الوصولِ (Access Control)،
المصادقةُ (Authentication)،
التوقيعُ الرَّقْميُّ (Digital Signature)،
سياساتُ الخصوصيةِ (Privacy Policies).

نتاجاتُ التعلُّمِ (Learning Outcomes)

- أصفُ وسائلَ الحمايةِ التي تحدُّ منْ مشكلاتِ مشاركةِ البياناتِ.
- أقيمَ وسائلُ الحمايةِ منْ حيثُ فعاليتُها والجدوى منْ استخدامِها وتأثيرِها الأخلاقيِّ.
- أناقشُ العلاقةَ بينَ فعاليةِ وسائلِ الحمايةِ، وجدواها، وتأثيرِها الأخلاقيِّ.

في عالمٍ رقميٍّ متسارعٍ، تظهرُ تطبيقاتٌ وأدواتٌ تسهلُ حياتَنا، وفي المقابلِ تزدادُ خطورةُ الانفتاحِ وانعدامُ الخصوصيةِ، وسهولةُ الوصولِ واختراقُ البياناتِ. فكيفَ أحمي بياناتِي في العالمِ الرقميِّ؟

نشاط تمهيدي

أتخيَّلُ نفسي المسؤولَ في كلِّ حالةٍ منَ الحالاتِ الآتيةِ، ثمَّ أجيبُ عنِ السؤالِ، ماذا أفعلُ لَو؟

- تلقيتُ بريدًا إلكترونيًا يحتوي على رابطٍ يبدو أنَّهُ منْ مصرفي، يطلبُ مني تسجيلَ الدخولِ لتأكيدِ معلوماتِ حسابي.
- وصلَني رابطٌ على الواتسآب منْ صديقِي المقربِ، يطلبُ الانضمامَ إلى مجموعةٍ خاصةٍ.
- نسيتُ كلمةَ المرورِ للدخولِ إلى حسابِ Gmail الخاصِّ بي.

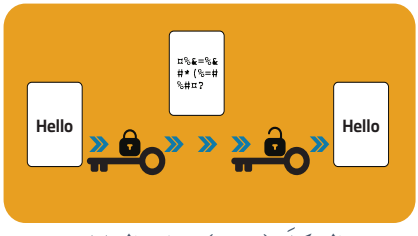
أناقشُ الإجاباتِ معَ الزملاءِ وأستمعُ لإجاباتِهمْ.

وسائلُ الحمايةِ التي تحدُّ منْ مشكلاتِ مشاركةِ البياناتِ

تهدفُ وسائلُ حمايةِ البياناتِ إلى تأمينِ معلوماتِنا منَ الوصولِ غيرِ المصرحِ بهِ، والتعديلِ، والسرقةِ، وغيرِها منَ المخاطرِ. يشملُ ذلكَ مجموعةً متنوعةً منَ التقنياتِ والممارساتِ التي تحدُّ منْ مشكلاتِ مشاركةِ البياناتِ.

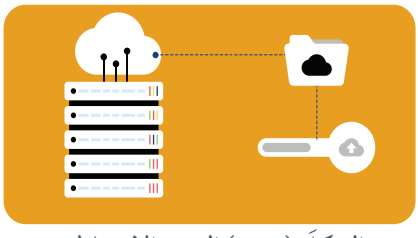
نذكرُ منها:

- **تشفيرَ البياناتِ (Encryption)**: وهيَ عمليةٌ تُحَوَّلُ عنْ طريقِها البياناتُ إلى صيغةٍ غيرِ قابلةٍ للقراءةِ إلا عبرَ مِفتاحِ تشفيرٍ محددٍ. انظرِ الشكلَ (4-1). وستُوضَّحُ بالتفصيلِ في الدرسِ القادمِ.



الشكلَ (4-1) تشفير البيانات

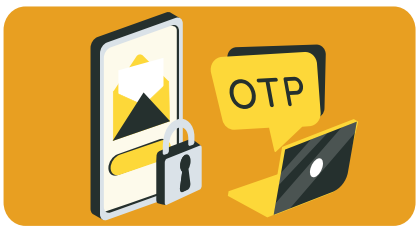
- **النسخَ الاحتياطيَّ (Backup and Recovery)**: يضمنُ النسخُ الاحتياطيَّ وجودَ نُسخٍ من البياناتِ للرجوعِ إليها عندَ فقدانِ البياناتِ أوْ إتلافِها؛ وذلكَ عنْ طريقِ إنشاءِ نسخٍ للبياناتِ وتخزينِها في مكانٍ آمنٍ، تمكِّنُ المؤسساتِ منْ استردادِ بياناتِها بسرعةٍ عندَ وقوعِ أيِّ خسارةٍ أوْ تلفٍ لبياناتِها.


الشكلَ (4-2) النسخ الاحتياطي

- **ضبطَ صلاحياتِ الوصولِ (Access Control)**: وهيَ عمليةُ منحِ صلاحياتٍ معينةٍ للأشخاصِ أوِ الجهاتِ المخوَّلةِ فقطْ بالوصولِ إلى البياناتِ.


الشكلَ (4-3) ضبط صلاحيات الوصول

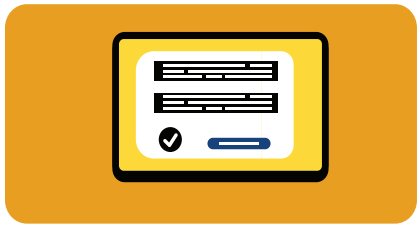
- **المصادقـــةَ (Authentication)**: وهيَ عمليةُ التأكدِ منْ هويةِ الأفـــرادِ أوِ الأجهزةِ التي تطلبُ الوصـــولَ إلى بياناتٍ معينةٍ قبلَ أنْ يمنحوا حقَّ الوصولِ إلى هـــذهِ البياناتِ، فمثلاً عندما يريدُ المستخدمُ الدخولَ إلى صفحتِهِ على الفيس بوك عنْ طريقِ جهازِ حاسوبٍ آخرَ، سيطلبُ منهُ الموقعُ رمزَ التأكيدِ، بأنَّ الشخصَ الذي يريدُ الدخولَ إلى صفحتِهِ هوَ نفسُهُ، ويرسلُ لهُ الرمزُ إما على الهاتفِ الجوالِ في رســـالةٍ، أوْ عبرَ البريدِ الإلكترونيِّ.



وتشملُ:

- **المصادقةَ الثنائيـــةَ (Two-Factor Authentication – 2FA)**: التي تَســـتخدمُ خطوتينِ أوْ عاملينِ؛ للتحقّقُ منْ هُويّةِ المستخدمِ عندَ تسجيلِ الدخولِ أوِ الوصولِ إلى خدمةٍ ما؛ حيثُ إنَّ الاعتمادَ على كلمةِ المرورِ فقطْ، قدْ لا يكونُ كافيًا. وبإضافةِ خطوةٍ ثانيةٍ، يصبحُ منَ الصعبِ على المهاجمينَ الوصولُ إلى الحساباتِ، ولوْ تمكّنوا منَ الحصولِ على كلمةِ المرورِ.
- **المصادقةَ الثلاثيـــةَ (Three-Factor Authentication – 3FA)**: حيثُ تتطلبُ ثلاثةَ عواملَ مختلفةٍ للتحققِ منْ هُويّةِ المســـتخدمِ، وهيَ بذلكَ تضيفُ طبقةَ أمانٍ أُخرى عبرَ الجمْعِ بينَ ثلاثةِ أنواعٍ مختلفةٍ منَ العواملِ.

- **التوقيعَ الرَّقْميَّ (Digital Signature)**: وهيَ تِقْنيةٌ تُستخدمُ للتأكُّدِ منَ البياناتِ وســـلامتِها عبرَ التوقيعِ بوساطةِ مفاتيحَ خاصةٍ.



- **سياساتِ الخصوصيةِ (Privacy Policies)**: هيَ سياساتٌ تحدِّدُ طرقَ جمعِ البياناتِ واستخدامِها ومشاركتِها، وتُلزَمُ المؤسســـاتِ باتِّباعِ هذهِ السياســـاتِ لحمايةِ خصوصيةِ الأفرادِ.

أناقش

أناقشُ معَ زملائِي تجربتِي الشـــخصيةَ معَ المصادقةِ الثنائيـــةِ أوِ الثلاثيةِ عنْ طريقِ التعاملِ معَ بريدِي الإلكترونيِّ أوِ الفيســـبوك، أوْ عندَ الدخولِ إلى حساباتِي على جوجل درايف أوْ مايكروسوفت.

نشاط فردي

أحلِّلُ وألخِّصُ:

أتأملُ سياســـةَ الخصوصيةِ الخاصةِ بموقعِ وزارةِ الاقتصادِ الرقميِّ والريادةِ في الأردنِّ الشكلِ (4-4)، وأقرؤُها جيدًا، ثمَّ ألخصُ النقاطَ الأساســيةَ التي تمثلُ حمايةَ البياناتِ، وأشاركُها معَ الزملاءِ في الصفِّ:

الشكلُ (4-4): سياسةُ الخصوصيةِ لوزارةِ الاقتصادِ الرَّقْميّ والريادةِ.

نشاط فردي

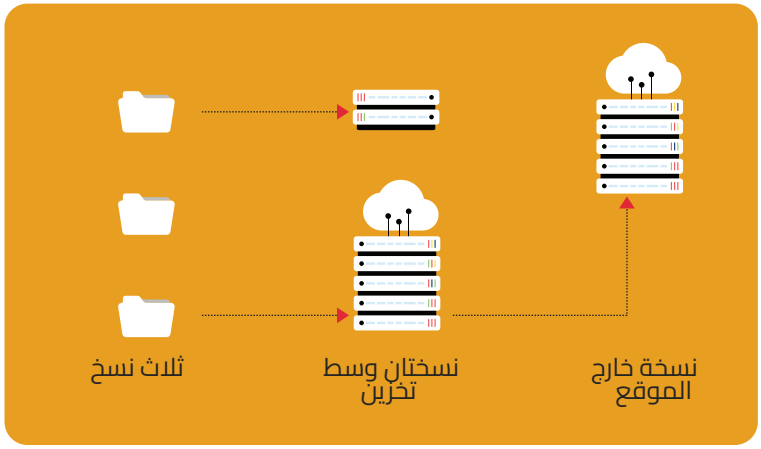
أفكِّرُ في وسائلِ حمايةِ البياناتِ السابقةِ، وأبينُ رأيِي الخاصَّ في استخدامِها أوْ عدمِ استخدامِها، وأذكرُ تأثيرَ تطبيقِها في خصوصيةِ بياناتِي معَ التبريرِ. أشـــاركُ أفكارِي معَ الزملاءِ في الصفِّ، وأناقشُهمْ بآرائِهمْ وأفكارِهمْ.

ولكنْ، هلْ تختلفُ هذهِ الطرقُ منْ حيثُ فعاليتُها والجدوى منْ اســـتخدامِها وتأثيرُها الأخلاقيِّ؟ كيفَ أختارُ الطريقةَ الفضلى؟ هلْ يجبُ أنْ أطبقَها جميعَها؟

هنـــاكَ اتفاقٌ على أنَّهُ لا توجدُ طريقةٌ واحدةٌ مثاليةٌ وكاملةٌ لحمايـــةِ البياناتِ، فقدْ لا يكونُ منَ الممكنِ تنفيذُ توصياتِ الأمنِ الســـيبرانيِّ الممكنةِ كافةً، ولكنْ على المؤسســـاتِ والأفرادِ تطبيقُ مجموعةٍ منَ الأساليبِ والتوصياتِ الفعالةِ التي تناســـبُ الموارِدَ والاحتياجاتِ، آخذينَ بعينِ الاعتبارِ فعاليةَ هذهِ الطرقِ وجدواها وتأثيرَها الأخلاقيِّ. ولا يعني تطبيقُ جميعِ الطرقِ أنَّ المؤسسةَ أوْ الفردَ بمأمنٍ منَ الهجماتِ السيبرانيةِ؛ ولكنَّ إعطاءَ الأولويةِ لبعضِ التوصياتِ التي تعالَجُ أعلى المخاطرِ لدى المؤسسةِ أوْ الفردِ، سوفَ يعملُ على التقليلِ منَ الهجماتِ الأمنيةِ بشكلٍ كبيرٍ. ويبينُ الجدولُ الآتي مقارنةً بينَ بعضِ الطرقِ منْ حيثُ الفعاليةَ والجدوى والتأثيرَ الأخلاقيَّ.

الطريقةُ	الفعاليةُ	الجدوى	التأثيرُ الأخلاقيُّ
التشفيرُ	يوفرُ التشفيرُ مســـتوىً عاليًا منَ الأمـــانِ، حتى لوْ حـــدثَ خرقٌ للبياناتِ، فإذا سُـــرقتْ البياناتُ المشـــفرةُ أوْ تمَّ الوصـــولُ إليها بطريقةٍ غيـــرِ مصرحـــةٍ، فإنَّها ســـتكونُ غيرَ قابلةٍ للقراءةِ، ومنْ ثمَّ ســـتكونُ عديمـــةَ الفائدةِ. **تعتمـــدُ فعاليةُ عمليةِ التشـــفيرِ على عوامـــلَ عدةٍ منهـــا:** نوعُ خوارزميةِ التشـــفيرِ المستخدمةِ وقوتُها، وحجمُ مفتاحِ التشـــفيرِ المســـتخدمِ ونوعُهُ، وســـريةُ مفتاحِ التشـــفيرِ، وكميةُ البياناتِ التي ســـيتمُّ تشـــفيرُها ونوعُها.	قدْ تكونُ عمليةُ التشـــفيرِ معقدةً ومكلفـــةً لتطبيقِها وصيانتِهـــا، وقدْ تســـببُ انخفاضًا في ســـرعةِ نقلِ البيانـــاتِ، وقلـــةِ كفاءةِ زمنِ الوصولِ والازدحامِ فـــي الشـــبكةِ وزيادتِهِ.	يمكنُ أنْ يتعارضَ التشفيرُ معَ القوانينِ واللوائحِ الخاصةِ، وحقوقِ الأفرادِ المختلفينَ؛ لذا يجـــبُ اســـتخدامُهُ بطريقةٍ تتوافقُ معَ القوانينِ واللوائحِ المحليةِ والدوليةِ. يجبُ أخـــذُ موافقةِ الأفرادِ والحصولُ على موافقتِهِمْ، وإخبارُهـــمْ أنَّ بياناتِهِمْ قدْ تعالجُ باســـتخدامِ التشفيرِ.
النسخُ الاحتياطيُّ	تســـمحُ للمؤسســـاتِ بالتعافي الســـريعِ منْ فقدانِ المعلوماتِ؛ باستردادِ بياناتِها بشكلٍ سريعٍ؛ مما يقللُ منْ وقتِ التوقفِ عنِ العملِ. توفيرُ طبقةٍ إضافيـــةٍ منَ الأمانِ؛ حيثُ يمكنُ استخدامُها لاستعادةِ البياناتِ منْ نقطةٍ زمنيةٍ محددةٍ؛ مما يســـاعدُ علـــى التراجعِ عنْ أيِّ خطأٍ، أوْ حـــذفٍ تمَّ مؤخرًا.	يكونُ النســـخُ الاحتياطيُّ ناجحًا وفعـــالًا إذا كانتِ البيئـــةُ التي توضـــعُ فيها النُسخُ الاحتياطيةُ ناجحةً وآمنـــةً، بالإضافـــةِ إلى أنَّهُ يجبُ اختبارُ النســـخِ الاحتياطيةِ بانتظامٍ؛ للتأكدِ مـــنْ إمكانيةِ اســـتعادتِها بنجاحٍ عندَ وقوعِ أيِّ كارثةٍ.	قبلَ إجراءِ النسخِ الاحتياطيِّ يجـــبُ أخـــذُ موافقـــةِ المســـتخدمينَ على عمليةِ جمعِ البياناتِ واستخدامِها ونســـخِها. ويجبُ تخزينُ نَسْخِ البياناتِ الاحتياطيِّ في مكانٍ آمنٍ ومحميٍّ، وضمانُ أنَّ الوصولَ إليها مقتصرٌ فقطْ على الأشخاصِ المخوَّلينَ.

 **ضبطُ صلاحياتِ الوصولِ** (Access Control)	تساعدُ في إنشاءِ المساءلةِ داخلَ المؤسساتِ عنْ طريقِ تمكينِها منْ تتبعِ منْ يمكنُهُ الوصولُ إلى الموارِدِ ومنْ نفذَ الإجراءاتِ ومراقبتِهِ؛ مما يقللُ منْ مخاطرِ التهديداتِ الداخليةِ.	يجبُ تنفيذُ ضبطِ صلاحياتِ الوصولِ بشكلٍ صحيحٍ حتى يكونَ فعالًا، فمثلًا يجبُ أنْ تكونَ كلماتُ المرورِ قويةً وفريدةً من نوعِها، ويجبُ تحديثُ أنظمةِ التحكمِ في الوصولِ واختبارُها بانتظامٍ للتأكدِ منْ أنَّها تعملُ بشكلٍ صحيحٍ.	يجبُ تطبيقُ ضبطِ صلاحياتِ الوصولِ بطريقةٍ تضمنُ العدالةَ بمنحِ صلاحياتِ الوصولِ للأشخاصِ منْ دونِ تمييزٍ أوْ تفضيلٍ. ويجبُ تحديدُ منْ يحصلُ على صلاحياتِ الوصولِ لأيِّ نوعٍ منَ البياناتِ، ولأيِّ سببٍ.
 **المصادقةُ** (Authentication)	تشكلُ المصادقةُ خطَّ الدفاعِ الأولِ في مواجهةِ التهديداتِ السيبرانيةِ، ولكنْ يجبُ الأخذُ بعينِ الاعتبارِ بعضَ الأمورِ لضمانِ فعاليةِ هذهِ الطريقةِ، مثلَ المصادقةِ متعددةِ العواملِ (MFA) التي تضيفُ طبقةَ أمانٍ إضافيةً، تتضمنُ معلوماتٍ شخصيةً، مثلَ كلمةِ المرورِ ومعلوماتٍ حولَ شيءٍ ماديٍّ كجهازِ الهاتفِ، ومعلوماتٍ بيولوجيةٍ كبصمةِ الوجهِ أوْ الصوتِ.	توجدُ تكاليفُ محتملةٌ مرتبطةٌ بتنفيذِ المصادقةِ. بشكلٍ عامٍّ قدْ يكلفُ حلُّ المصادقةِ الثنائيةِ البسيطِ (2FA) الذي يستخدمُ رسائلَ SMS للتحققِ بضعةَ دولاراتٍ شهريًا. أما حلُّ المصادقةِ الثنائيةِ الأكثرِ تعقيدًا والذي يستخدمُ الرموزَ المميزةَ للأجهزةِ، والمصادقةَ البيولوجيةَ كبصمةِ الوجهِ، فقدْ يكلفُ مئاتِ الدولاراتِ شهريًا.	يتطلبُ تطبيقُ المصادقةِ مراعاةَ المبادئِ الأخلاقيةِ التي تتعلقُ بالشفافيةِ، وحمايةِ المعلوماتِ، وموافقةِ المستخدمِ



الشكل (4-5) : صورةٌ توضيحيةٌ لإستراتيجيةِ النسخِ الاحتياطيِّ 3-2-1

إضاءةٌ

يوصي الخبيرونَ باستخدامِ طريقةِ 3-2-1 للنسخِ الاحتياطيِّ (Data Backup Method 3-2-1)، وتعني نسخَ البياناتِ ثلاثَ نسخٍ احتياطيةٍ على جهازينِ محليينِ (الجهازِ الأصليِّ، وقرصٍ صلبٍ خارجيٍّ) وموقعٍ خارجيٍّ واحدٍ (سحابةٌ). انظرِ الشكلَ (4-5).

أناقش

أناقشُ معَ زملائي فـــي المجموعةِ طرقَ حمايةِ البياناتِ الواجـــبِ تطبيقُها في كلِّ حالةٍ منَ الحالاتِ الآتيةِ، وترتيبُها وَفقَ الأولويَّةِ:

الحالةُ	طرقُ حمايةِ البياناتِ مرتبةً بحسبِ الأولويَّةِ
استخدامُ شبكةِ Wi-Fi عامةً.	.....
تلقي بريدٍ إلكترونيٍّ منْ مصدرٍ غيرِ معروفٍ.	.....
تخزينُ معلوماتٍ حساسةٍ على جهازِ الحاسوبِ.	.....
تنزيلُ تطبيقٍ منَ الإنترنت.	.....
الموظفونَ يعملونَ عنْ بعدٍ.	.....
جمـــعُ البياناتِ الشـــخصيةِ للعملاءِ لأغراضِ التسويقِ.	.....
استخدامُ أجهزةِ USB خارجيةٍ في الشركةِ.	.....

نشاط جماعي

مناقشةُ العلاقةِ بينَ فعاليةِ وسائلِ حمايةِ البياناتِ وتحليلِها، وجدواها وأثرِها الأخلاقيِّ

أتعاونُ معَ زملائِي ضمنَ المجموعةِ لاستكشافِ كيفيةِ تأثيرِ وسائلِ حمايةِ البياناتِ في الأمانِ الإلكترونيِّ والأخلاقياتِ المهنيةِ، والبحثِ ومناقشةِ فعاليةِ هذهِ الوسائلِ ومدى جدواها، والتركيزِ على تأثيرِها الأخلاقيِّ في المستخدمينَ والمجتمعِ، ثمَّ تقديمِ أمثلةٍ واقعيةٍ توضحُ كيفيةَ تطبيقِ هذهِ الوسائلِ، وما التحدياتُ التي تواجهُها. ونشاركُ ما نتوصلُ إليهِ منْ أفكارٍ ونتائجَ معَ زملائِنا في المجموعاتِ الأخرى، ونستمعُ إلى آراءِ الآخرينَ وأفكارِهمْ، ونناقشُهمْ لتعميقِ الفهمِ المشتركِ.

المواطنةُ الرَّقْميّةُ

- **الخصوصيةُ وحمايةُ البياناتِ الشخصيةِ**: حمايةُ البياناتِ الشخصيةِ والخصوصيةِ في أثناءِ استخدامِ التكنولوجيا، وتوخي الحذرِ في مشاركةِ المعلوماتِ الشخصيةِ عبرَ الإنترنت.
- **الأمنُ الرقميُّ**: استخدامُ برامجِ مكافحةِ الفيروساتِ، وتطبيقاتِ الحمايةِ، وتحديثُ الأنظمةِ بانتظامٍ لضمانِ عدمِ وجودِ ثغراتٍ يمكنُ استغلالُها.
- **المسؤوليةُ الرقميةُ**: الالتزامُ بممارساتٍ آمنةٍ ومسؤولةٍ على الإنترنت، واحترامُ حقوقِ الآخرينَ في الفضاءِ الرقميِّ.
- الامتناعُ عنْ التصرفاتِ الضارةِ، مثلَ اختراقِ الأنظمةِ أوْ سرقةِ البياناتِ، والحرصِ على التعاملِ معَ المعلوماتِ بحذرٍ ومسؤوليةٍ.
- **الشفافيةُ في التعاملِ معَ البياناتِ**: الوعيُ بكيفيةِ استخدامِ البياناتِ منْ قِبلِ المواقعِ والخدماتِ التي يستخدمونَها، وقراءةُ سياساتِ الخصوصيةِ للمواقعِ الإلكترونيةِ قبلَ استخدامِ خدماتِها، واختيارُ الخدماتِ التي تحترمُ حمايةَ البياناتِ الشخصيةِ.
- **الاستخدامُ القانونيُّ للتكنولوجيا**: اتباعُ القوانينِ المتعلقةِ بحمايةِ البياناتِ والأمنِ السيبرانيِّ، والامتثالُ للقوانينِ المحليةِ والدوليةِ المتعلقةِ بحمايةِ البياناتِ، مثلَ قوانينِ الجرائمِ الإلكترونيةِ، وقوانينِ حمايةِ الخصوصيةِ.

المشروعُ: حملةٌ إعلاميّةٌ توعويّةٌ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ/ مهمة 4

أتعـــاونُ معَ زملائي لإنتاجِ المهمةِ الرابعةِ في الموادِّ التوعويةِ التي تتمحورُ حولَ إعدادِ خريطةٍ ذهنيةٍ تفاعليةٍ (Interactive Mindmap) عنْ وسائلِ حمايةِ البياناتِ باستخدامِ أداةِ (Coggle)، للمشاركةِ في حملةٍ توعويةٍ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ، بحيثُ تحتوي الخريطةُ الذهنيةُ التفاعليةُ التشاركيةُ على تفرعاتٍ توضحُ كلَّ وسيلةٍ لحمايةِ البياناتِ، معَ شرحٍ مختصرٍ وصـــورٍ توضيحيةٍ، بالإضافةِ إلى عناصرَ تفاعليةٍ وروابطَ خارجيـــةٍ. وأنْ تكونَ قابلةً للتنزيلِ بصيغةِ (PDF)، عبرَ اتباعِ الخطواتِ الآتيةِ:

- **تحديدِ العنوانِ الرئيسِ للخريطةِ الذهنيةِ**: العنوانُ الرئيسُ هوَ "وسائلُ حمايةِ البياناتِ"..
- **باستخدامِ أداةِ (Coggle) التي يمكنُ الوصولُ إليها عبرَ الرابطِ الآتي**: https://coggle.it/ ، أوْ عنْ طريقِ مســـحِ رمزِ الاســـتجابةِ السريعِ المجاورِ، أوْ يمكنُ اســـتخدامُ أيِّ أداةٍ رقميةٍ أخرى لرسمِ الخرائطِ الذهنيةِ التي ألفَها.
- **إنشاءِ تفرعاتٍ**: إضافةُ تفرعاتٍ منَ العنوانِ الرئيسِ؛ بحيثُ يمثلُ كلُّ تفرعٍ وسيلةً معينةً منْ وسائلِ حمايةِ البياناتِ، مثلَ التشفيرِ، وكلماتِ المرورِ القويةِ، والجدرانِ الناريةِ، والتحققِ بخطوتينِ.
- **إدراجِ شرحٍ مختصرٍ وصورٍ**: تحتَ كلِّ تفرعٍ، يُكتبُ شرحٌ بسيطٌ، يوضحُ كلَّ وسيلةٍ لحمايةِ البياناتِ، معَ إدراجِ صورٍ ذاتِ علاقةٍ لتعزيزِ الفهمِ.
- **إضافةِ عناصرَ تفاعليةٍ**: إضافةُ روابطَ تفاعليةٍ لعناصرَ خارجيةٍ تحتوي على معلوماتٍ حولَ وسائلِ حمايةٍ إضافيةٍ لمْ تذكرْ في الدرسِ؛ مما يثري المعلوماتِ الموجودةَ في الخريطةِ.
- **تنزيلِ الخريطةِ الذهنيةِ بصيغةِ (PDF)**: بعدَ إتمامِ الخريطةِ، يتمُّ تنزيلُها على شـــكلِ ملفِّ (pdf)؛ ليتمكنَ الطلبةُ منْ مراجعتِها بسهولةٍ.
- **مشاركةُ الخريطةِ الذهنيةِ**: عرضُ الخريطةِ الذهنيةِ على زملاءِ الصفِّ، ومناقشةُ الوسائلِ المختلفةِ لحمايةِ البياناتِ.

الالتزامِ بالنصائحِ الآتيةِ عندَ التصميمِ::

- الدقةُ في المعلوماتِ والوضوحِ.
- البساطةُ في التصميمِ والشرحِ المختصرِ.
- استخدامُ عناصرَ تفاعليةٍ مثلِ الروابطِ لإثراءِ الخريطةِ.

مشروع

أقيّمُ تعلّمي

المعرفةُ: أوظفُ في هذا الدرسِ ما تعلّمتُهُ منْ معارفَ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: أكتبُ المصطلحَ العلميَّ المناسبَ لكلِّ جملةٍ منَ الجملِ الآتيةِ:

- عمليةُ تحويلِ البياناتِ إلى صيغةٍ غيرِ قابلةٍ للقراءةِ. ( )
- إنشاءُ نسخٍ عندَ فقدانِ البياناتِ أوْ إتلافِها وتخزينُها في مكانٍ آمنٍ، تمكنُ المؤسساتِ منِ استردادِ بياناتِها بسرعةٍ. ( )
- منحُ أذوناتٍ معينةٍ للأشخاصِ أوِ الجهاتِ المعنيةِ فقطْ للوصولِ إلى البياناتِ. ( )
- التأكدُ منْ هويةِ الأفرادِ أوْ الأجهزةِ التي تطلبُ الوصولَ إلى بياناتٍ معينةٍ. ( )

السؤالُ الثاني: أقارنُ بينَ طريقتيِ التشفيرِ والنسخِ الاحتياطيِّ منْ حيثُ الفعاليةُ والجدوى والتأثيرُ الأخلاقيُّ.

.....

.....

.....

.....

السؤالُ الثالثُ: أختارُ طريقةَ حمايةِ البياناتِ المناسبةِ لكلِّ حالةٍ منَ الحالاتِ الآتيةِ:

- منعِ وصولِ الأشخاصِ غيرَ المصرحِ لهمْ إلى البياناتِ.

.....

.....

- ضمانِ توفيرِ البياناتِ واستعادتِها عندَ حدوثِ فقدانٍ أوْ تلفٍ للبياناتِ الأصليةِ.

.....

.....

- حمايةِ البياناتِ منَ الوصولِ غيرِ المصرحِ بهِ عندَ نقلِ البياناتِ عبرَ الشبكاتِ.

.....

.....

- تحديدِ الأذوناتِ، وتنظيمِ الوصولِ، ومنعِ الوصولِ غيرِ المصرحِ بهِ.

.....

.....

المهاراتُ: أوظّفُ مهاراتِ التفكيرِ الناقدِ والتواصلَ الرَّقْميَّ والبحثَ الرَّقْميَّ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: باستخدامِ مهارةِ البحثِ الرقميِّ أبحثُ في مواقعِ الإنترنت الآمنةِ عنِ القانونِ الأردنيِّ لحمايةِ البياناتِ الشخصيةِ، وألخصُ أهمَّ النقاطِ على شكلِ بوسترٍ باستخدامِ برنامجِ CANVA، وأنشرُهُ على صفحةِ المدرسةِ على مواقعِ التواصلِ الاجتماعيِّ.

السؤالُ الثاني: معَ التطورِ المتسارعِ في العصرِ الرقميِّ وظهورِ الذكاءِ الاصطناعيِّ، كيفَ أتخيلُ مستقبلَ التعاملِ معَ البياناتِ الرقميةِ وحمايتِها؟ هلْ أتوقعُ استحداثَ طرقٍ جديدةٍ لنقلِها بأمانٍ؟ أدونُ توقعاتِي وأشاركُها معَ الزملاءِ.

.....

.....

.....

القِيَمُ والاتجاهاتُ:

أبحثُ في أهمِّ المبادئِ والقيمِ الأخلاقيةِ التي تتوافقُ معَ ممارساتِ الأمنِ السيبرانيِّ، وتلكَ التي تتعارضُ معها، وأضعُها في جدولٍ على برنامجِ ميكروسوفت وورد Word، وأشاركُها معَ زملائِي في الصفِّ.

الدرسُ الخامسُ

التَّشفيرُ
(Encryption)

الفكرةُ الرئيسةُ:

التعرُّفُ إلى مفهومِ تشـــفيرِ البياناتِ وأهميتِهِ في حمايةِ هذهِ البياناتِ، والتعرفُ إلى الطرقِ البســـيطةِ والمعقدةِ للتشفيرِ، وتطبيقُ عملياتِ التشـــفيرِ وفكِّ التشـــفيرِ باستخدامِ طرقٍ ومستوياتِ صعوبةٍ مختلفةٍ

المفاهيمُ والمصطلحاتُ:

التشـــفيرُ (Encryption)، فـــكُّ التشـــفيرِ (Decryption)، خوارزمياتُ التعويضِ (Substitution)، خوارزمياتُ الإبدالِ (Transposition)، خوارزميةُ المنتَجِ (Product)، شيفرةُ قيصرَ (Caesar Cipher)، شـــيفرةُ تبديلِ سياجِ الســـكةِ الحديديةِ (Rail Fence Transposition Cipher)، المفتـــاحُ الخـــاصُّ (Private Key)، التشفيرُ المتماثِلُ (Symmetric Encryption)، المفتـــاحُ العـــامُّ (Public Key)، التشـــفيرُ غيـــرُ المتماثِلِ (Asymmetric Encryption) ، تشفيرُ الكتلِ (Block Cipher)، تشفيرُ التدفُّقِ (Stream Cipher).

نتاجاتُ التعلُّمِ (Learning Outcomes)

- أعرِّفُ عمليةَ تشفيرِ البياناتِ وأهميتَها للحمايةِ.
- أوضّحُ الطرقَ البسيطةَ والمعقدةَ لتشفيرِ البياناتِ.
- أشرحُ إطارَ العملِ لتشفيرِ البياناتِ.
- أطبقُ عملياتِ التشفيرِ وفكِّ التشفيرِ باستخدامِ طرقٍ ومستوياتِ صعوبةٍ مختلفةٍ.

منتجاتُ التعلُّمِ
(Learning Products)

إنتاجُ المطويـــةِ الإلكترونيةِ التفاعليةِ "مغامراتُ التشفيرِ؛ رحلتُكَ في أمـــانِ البياناتِ" باستخدامِ أداةِ (Canva)، ضمنَ التحضيـــراتِ لحملةٍ توعويةٍ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ.

هناكَ كمياتٌ كبيرةٌ منَ البياناتِ الحساسةِ والمهمةِ المخزنةِ على أجهزةِ الحواسيبِ، وتُنقلُ بينَ الأجهزةِ يوميًا، بما فيها منْ كلماتِ مرورٍ وحساباتٍ ومعلوماتٍ ماليةٍ ومعلوماتٍ شخصيةٍ. ولحمايةِ هذهِ البياناتِ وإبقائِها مخفيةً عنْ طرفٍ ثالثٍ قدْ يسعى لسرقتِها، ومعَ تزايدِ الهجماتِ السيبرانيةِ، وتعقيدِها وتكرارِها، أصبحتْ توصياتُ الأمنِ السيبرانيِّ ضروريةً لأيِّ مؤسسةٍ لحمايةِ بياناتِها، ويعدُّ التشفيرُ منَ العناصرِ الأساسيةِ للأمنِ السيبرانيِّ. فما التشفيرُ؟ وما طرقُهُ؟

نشاط تمهيدي

يريدُ أحمدُ إرسالَ رسالةٍ سريةٍ مكتوبةٍ إلى صديقِهِ عليٍّ عنْ طريقِ أحدِ المعارفِ، ولكنَّ أحمدَ لا يضمنُ عدمَ قراءةِ الرسالةِ منَ الشخصِ الناقلِ. كيفَ يضمنُ أحمدُ سريةَ الرسالةِ إلى حينِ وصولِها إلى عليٍّ؟ أقترحُ بعضَ الأفكارِ التي تحفظُ رسالةَ أحمدَ، وإنْ فُتحتْ فعلًا. وأناقشُها معَ الزملاءِ.

مفهومُ التشفيرِ

يُعرَّفُ التشفيرُ بأنَّهُ عمليةُ تحويلِ النصِّ الأصليِّ إلى نصٍّ غيرِ مفهومٍ إلا منْ قِبلِ الشخصِ المرسِلِ والشخصِ المستقبلِ للرسالةِ؛ بهدفِ إخفاءِ معلوماتِ الرسالةِ الأصليةِ وجعلِها غيرَ مقروءةٍ أوْ مفهومةٍ للمستلمينَ غيرِ المقصودينَ بالرسالةِ بما يضمنُ حمايتَها. إنَّ فكرةَ التشفيرِ ليستْ فكرةً جديدةً وجدتْ في العصرِ الرقميِّ والثورةِ التكنولوجيةِ، بلْ هيَ فكرةٌ موجودةٌ قبلَ إيجادِ شبكةِ الإنترنت بوقتٍ طويلٍ، ففي العصرِ الرومانيِّ شفرَ يوليوس قيصرَ رسائلَ إلى جنودِهِ بطريقةٍ معينةٍ.

وفي علومِ الحاسوبِ، يقومُ مبدأُ التشفيرِ على مجموعةٍ منَ المفاهيمِ الرياضيةِ لتحويلِ المعلوماتِ إلى معلوماتٍ يصعبُ فكُّ شيفرتِها؛ لحمايتِها منَ الاختراقِ والسرقةِ، وتُستخدمُ في تصفحِ مواقعِ الويبِ على شبكةِ الإنترنتْ، والتواقيعِ الرقميةِ، والاتصالاتِ السريةِ، مثلَ معاملاتِ بطاقاتِ الائتمانِ والبريدِ الإلكترونيِّ.

أبحثُ

أبحثُ في المواقعِ الإلكترونيّةِ الموثوقةِ عنْ نشأةِ التشفيرِ، وعنْ مواقفَ حقيقيةٍ استُخدمَ فيها التشفيرُ، وأشاركُ ما أتوصلُ إليهِ معَ الزملاءِ.

طرقُ تشفيرِ البياناتِ

هناكَ عديدٌ منْ خوارزمياتِ التشفيرِ وطرقِهِ، وهيَ تتفاوتُ في تعقيدِها وقوتِها. ومعظمُ خوارزمياتِ التشفيرِ الحديثةِ تتضمنُ عملياتٍ حسابيةً بمستوىً عالٍ منَ التعقيدِ. هناكَ أيضًا خوارزمياتُ تشفيرٍ بسيطةٌ لا تحتاجُ إلى عملياتٍ حسابيةٍ معقدةٍ، وإنَّما تحتاجُ بعضَ الإجراءاتِ البسيطةِ التي يستطيعُ معظمُ الأفرادِ تعلُّمَها بسهولةٍ.

ويمكنُ تصنيفُ خوارزمياتِ التشفيرِ بحسبِ ثلاثةِ معاييرَ، هيَ:

أولًا: بحسبِ نوعِ عمليةِ التشفيرِ المستخدَمةِ:

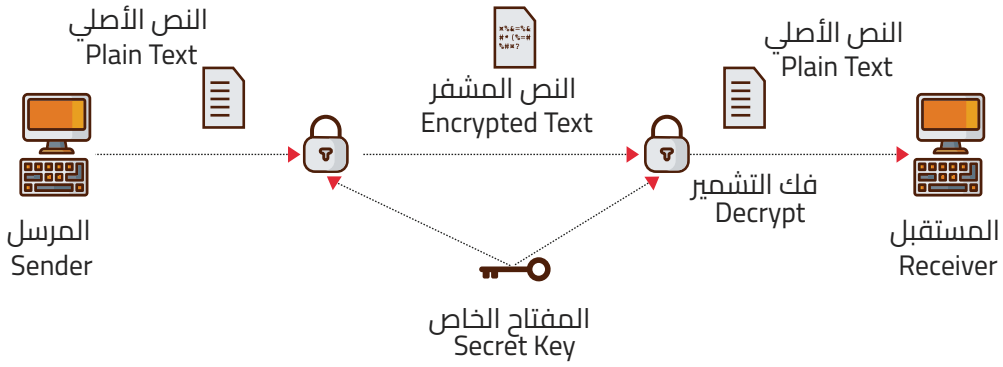
ومنْ أنواعِها:

- **خوارزمياتُ التعويضِ (Substitution)**: وهيَ الخوارزمياتُ التي تعتمدُ على تغييرِ حروفِ الرسالةِ بحروفٍ أخرى مثلَ شيفرةِ قيصرَ (Caesar Cipher).
- **خوارزمياتُ الإبدالِ (Transposition)**: وهيَ خوارزمياتٌ تعتمدُ على تبديلِ أماكنِ الحروفِ عنْ طريقِ إعادةِ ترتيبِ نصِّ الرسالةِ، مثلَ خوارزميةِ تبديلِ سياجِ السكةِ الحديديةِ (Rail Fence Transposition Cipher).
- **خوارزميةُ المنتجِ (Product)**: وهيَ خوارزمياتٌ تجمعُ بينَ تحويلينِ أوْ أكثرَ لتشفيرِ البياناتِ، وصممتْ لتوفيرِ مستوىً أعلى منَ الأمانِ مقارنةً بعملياتِ التشفيرِ التي تعتمدُ على تقنيةٍ واحدةٍ فقطْ للتشفيرِ. ويمكنُ لتشفيرِ المنتجِ أنْ يحتويَ على تشفيرٍ بالتعويضِ وتشفيرٍ بالإبدالِ معًا.

ثانيًا: بحسبِ مِفتاحِ التشفيرِ المُستخدَمِ:

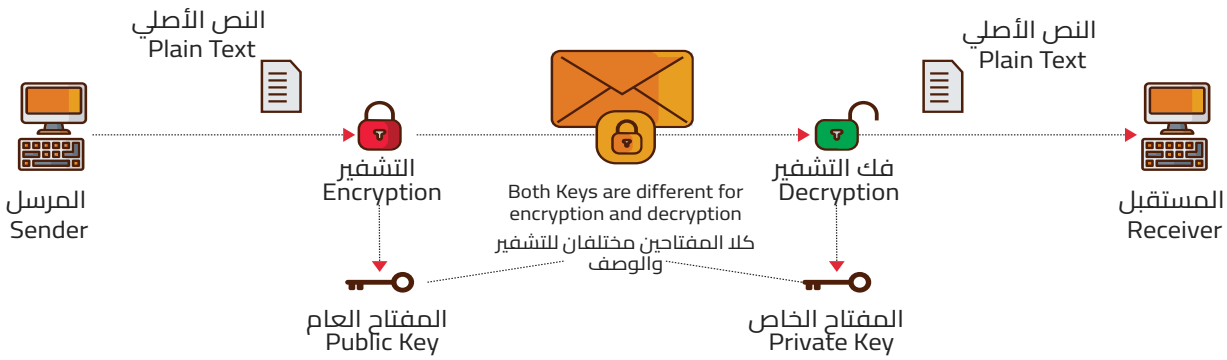
ومنْ أنواعِها:

- **التشـــفيرُ المتماثلُ (Symmetric Encryption)**: ويعرفُ هذا النهجُ في التشـــفيرِ أيضًا باســـم تشـــفيرِ المفتاحِ الخاصِّ (Private Key Cryptography)، وهيَ طريقةٌ في التشفيرِ يُستخدمُ فيها مفتاحٌ سريٌّ خاصٌّ واحدٌ لتشفيرِ النصِّ وفكِّ التشـــفيرِ، ويملكُ الوصولَ إلى هذا المفتاحِ كلٌّ منَ المرسلِ والمستقبلِ، ويَستخدمُ المرســـلُ والمستقبلُ المفتاحَ نفسَهُ للتشفيرِ وفكِّ التشفيرِ. يوضحُ الشـــكلُ (5-1) مبدأَ عملِ هذهِ التِّقْنيةِ في التشفيرِ. ألاحظُ أنَّ المِفتاحَ الخاصَّ هوَ نفسُهُ المستخدَمُ للتشفيرِ وفكِّ التشفيرِ.



الشكلُ (5-1) مبدأ عمل التشفير المتماثل

- **التشـــفيرُ غيرُ المتماثلِ (Asymmetric Encryption)**: ويعرفُ هذا النهجُ منْ التشفيرِ أيضًا باسم تشـــفيرِ المفتاحِ العامِّ (Public key Cryptography)، ويســـتخدمُ هنا مفتاحانِ للتشفيرِ؛ مفتاحٌ خاصٌّ (Private Key) ومفتاحٌ عامٌ (Public Key) ويَســـتخدمُ كلُّ طـــرفٍ منْ طرفيْ المحادثةِ (المســـتقبلِ والمرســـلِ) مفتاحًا مختلفًا؛ فالمفتاحُ العامُّ كما يوحي اســـمُهُ متاحٌ للجميعِ، أوْ يشاركُ معَ الأشـــخاصِ المســـتلمينَ المعتمدينَ، أما المفتاحُ الخاصُّ، فهوَ يُعطى لأشخاصٍ محددينَ فقطْ، ولا يُتـــاحُ للعامةِ، ومنْ يملكُهُ فقطْ هوَ منْ يســـتطيعُ فكَّ التشفير.التشـــفيرِ. يبينُ الشكلُ (5-2) مبدأَ عملِ هذا النهجِ منَ التشفيرِ.



الشكل (5-2): مبدأ عمل التشفير غير المتماثل

نشاط جماعي

نمذجةُ التشفيرِ

أتعاونُ معَ زملائي في المجموعةِ على اختيارِ إحدى طرقِ التشـــفيرِ (المتماثلِ، غيرِ المتماثلِ) وتنفيذِ ما يأتي:

- اختيارُ مجموعةٍ لتكونَ هيَ "المستقبلَ" ومجموعةً لتكونَ هيَ "المرسِلُ"
- كتابةُ نصِّ رسالةٍ سريٍّ.
- إنشاءُ مفتاحِ التشفيرِ (مفتاحٌ واحدٌ في حالةِ التشفيرِ المتماثلِ، ومفتاحانَ (عامٌ وخاصٌّ) في التشفيرِ غيرِ المتماثلِ).
- مشاركةُ مفتاحِ التشفيرِ معَ المجموعةِ (المستقبلِ).
- تشفيرُ نصِّ الرسالةِ ومشاركتُها معَ المجموعةِ (المستقبلِ).
- اختبارُ قدرةِ المجموعةِ (المستقبلِ) على معرفةِ نصِّ الرسالةِ الأصليِّ.

مناقشـــةُ المجموعاتِ في الفرْقِ بينَ التشـــفيرِ المتماثِلِ وغيرِ المتماثِلِ، منْ حيثُ الصعوبةُ في التشفيرِ أوْ فكُّ التشفيرِ، وفي أمانِ البياناتِ.

ثالثًا: بحسبِ طريقةِ معالجةِ النصِّ الأصليِّ:

ومنْ أنواعِها:

- تشفيرُ الكُتلِ (Block Cipher).
- تشفيرُ التدفُّقِ (Stream Cipher).

تختلفُ هذهِ الطرقُ بعضُها عنْ بعضٍ منْ حيثُ آليةُ العملِ والسرعةُ والأمانُ. يوضحُ الجدولُ (1-5) بعضَ الفروقِ بينَ خوارزمياتِ الكتلِ وخوارزمياتِ التدفقِ في التشفيرِ.

تشفيرُ الكُتَلِ Block Cipher	تشفيرُ التدفُّقِ Stream Cipher
تحوُّلُ النصُّ الأصليُّ إلى نصٍّ مشفرٍ بأخذِ النصِّ الأصليِّ مثلَ كتلةٍ في كلِّ مرةٍ (الكتلةُ تستخدمُ 64 بتّ أوْ أكثرَ.	تحوُّلُ النصُّ الأصليُّ إلى نصٍّ مشفرٍ بأخذِ بت واحدٍ من الرسالةِ الأصليةِ في كلِّ مرةٍ (شيفرةُ التدفقِ تستخدمُ 8 بت في كلِّ مرةٍ).
عمليةُ تشفيرِ الكتلِ بسيطةٌ.	عمليةُ تشفيرِ التدفقِ أكثرَ تعقيدًا.
عمليةُ فكِّ التشفيرِ صعبةٌ.	عمليةُ فكِّ التشفيرِ سهلةٌ.
يعملُ تشفيرُ الكتلِ على مبدأِ التشفيرِ بالإبدالِ (مثلَ تشفيرِ سياجِ السكةِ الحديديةِ).	يعملُ تشفيرُ التدفقِ على مبدأِ التشفيرِ بالتعويضِ (مثلَ شيفرةِ قيصرَ).
تستهلكُ وقتًا أطولَ مقارنةً بتشفيرِ التدفقِ.	تستهلكُ وقتًا أقلَّ.
أكثرُ أمنًا.	أقلُّ أمنًا.

جدولُ (1-5): مقارنةٌ بينَ تشفيرِ الكُتلِ وتشفيرِ التدفُّقِ منْ حيثُ آليةُ العملِ والسرعةُ والأمانُ

لنستعرضَ بشيءٍ منَ التفصيلِ آليةَ تطبيقِ بعضِ خوارزمياتِ التشفيرِ، ومنْها:

- **التشفيرُ بالتعويضِ**: وهيَ شيفرةٌ قصيرةٌ (Caesar Cipher).
- **التشفيرُ بالإبدالِ**: وهيَ شيفرةُ تبديلِ سياجِ السكةِ الحديديةِ (Rail Fence Transposition Cipher).

شيفرةُ قيصرَ (Caesar Cipher)

وهيَ إحدى أقدمِ خوارزمياتِ التشـــفيرِ وأكثرِها بســـاطةً، وهيَ من أنواعِ خوارزمياتِ التشفيرِ بالتعويضِ. وسميتْ بهذا الاســـمِ نسبةً إلى القائدِ الرومانيِّ يوليوس قيصر الذي استخدمَها لتشفيرِ الرســـائلِ إلى جنودِهِ؛ من أجلِ عدمِ كشفِ رسائلِهِ منَ العدوِّ، ويقومُ مبدؤُها على إزاحـــةِ الحروفِ الأبجديةِ عـــددًا محددًا منَ الإزاحاتِ لإنتاجِ نصٍّ جديدٍ غيرِ مفهومٍ

خطواتُ تطبيقِ الخوارزميّةِ:

- اختيارُ قيمةِ الإزاحةِ للحروفِ في الرسالةِ (حيثُ تتراوحُ قيمةُ الإزاحةِ بينَ 25 – 1).
- إنشاءُ جدولٍ منْ صفينِ؛ حيثُ يحتوي الصفُّ الأولُ منَ الجدولِ على الحروفِ بترتيبِها العاديِّ، ويحتوي الصفُّ الثاني على الحروفِ بعدَ تطبيقِ قيمةِ الإزاحةِ.
- تشفيرُ الرسالةِ بتغييرِ كلِّ حرفٍ فيها بالحرفِ الموجودِ في الصفِّ الثاني منْ الجدولِ بعدَ تطبيقِ الإزاحةِ.
- التأكدُ أنَّ مستلمَ الرسالةِ لديْهِ مفتاحُ الإزاحةِ حتى يستطيعَ فكَّ التشفيرِ.
- لفكِّ تشفيرِ الرسالةِ في شيفرةِ قيصرَ، تطبقُ المعادلةَ (25 – قيمةَ الإزاحةِ) لإيجادِ قيمةِ الإزاحةِ في النصِّ المشفرِ، وإعادةِ الحروفِ الأصليةِ.

تَستخدمُ شـــيفرةُ قيصرَ حروفَ اللغةِ الإنجليزيةِ، ولا يوجدُ فرقٌ بينَ الحروفِ الصغيرةِ والكبيرةِ، ولكنْ يفضلُ استخدامَ نوعٍ واحدٍ في كلِّ مرةٍ؛ إمّا استخدامُ حروفٍ كبيرةٍ أوْ حروفٍ صغيرةٍ.

مثال (1):

1. **أستخدمُ شيفرةَ قيصرَ لتشفيرِ الرسالةِ الآتيةِ، علمًا أنَّ مِفتاحَ الإزاحةِ هوَ 10:**

I Like chemistry

ننشـــئُ جدولًا مكوَّنًا منْ صفينِ؛ يحتوي الصفُّ الأولُ على الحـــروفِ بترتيبِها العاديِّ، ويحتوي الصفُّ الثاني على الحروفِ بعدَ تطبيقِ مِفتاحِ الإزاحةِ وهوَ 10؛ إذْ ســـتبدأُ بالحرفِ (k)؛ لأنَّنا نفذِّنْا إزاحـــةَ أولِ 10 حروفٍ هيَ a,b,c,d,e,f,g,h,I,j ، ومنْ ثمَّ الحرفَ الحادي عشـــرَ وهوَ (k)، ونكملُ الحـــروفَ في الصفِّ الثاني إلى أنْ نصلَ إلى الحرفِ (z). ثمَّ بعـــدَ ذلكَ نعودُ ونكملُ ما تبقّى منْ الصفِّ الثاني ابتداءً منَ الحرفِ (a).

كما هوَ مبينٌ في جدولِ التشفيرِ الآتي:

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

2. **نستخدمُ جدولَ التشفيرِ الناتجَ لتشفيرِ الرسالةِ:**

I Like Chemistry

فنلاحظُ أنَّ الحـــرفَ (i) في الصفِّ الأولِ منْ الجدولِ، يقابلُهُ الحـــرفُ (s) في الصفِّ الثاني منَ الجـــدولِ، وأنَّ الحرفَ (L) في الصفِّ الأولِ منَ الجدولِ، يقابلُهُ الحرفُ (v) في الصفِّ الثاني منَ الجدولِ. والحرفَ (k) يقابلُهُ الحرفُ (u) وهكذا.... ولتســـهيلِ نقلِ الحروفِ المشـــفرةِ للرسالةِ الأصليةِ ننشئُ جدولًا يحتوي على نصِّ الرسالةِ الأصليةِ في الصفِّ الأولِ، ثمَّ ننقلُ الحرفَ المشفرَ المكافئَ لهُ إلى الصفِّ الثاني،

كما هوَ مبينٌ في الجدولِ الآتي:

النص الأصلي	I		L	i	k	e		C	h	e	m	i	s	t	r	y
النص المشفر	s		v	s	u	o		m	r	o	w	s	c	d	b	I

فيكونُ النصُّ المشفَّرُ هوَ:

s vsuo mrowscdbi

نشاط عملي

أستخدمُ شيفرةَ قيصرَ لتشفيرِ النصِّ الآتي باستخدامِ مِفتاحِ إزاحةٍ بقيمةٍ 11.

Be kind to your parent

نشاط

أستخدمُ شيفرةَ قيصرَ لتشفيرِ اسمِ مدرستِي باستخدامِ مفتاحِ إزاحةٍ 22، وأقارنُ النصَّ المشفرَ الناتجَ معَ الزملاءِ، هلْ النتيجةُ هيَ نفسُها؟

مثال (2)

يبينُ المثالُ الآتي كيفيةَ فكِّ تشفيرِ رسالةٍ ما باستخدامِ شيفرةِ قيصرَ: لفكِّ شيفرةِ الرسالةِ الآتيةِ باستخدامِ شيفرةِ قيصرَ، علمًا بأنَّ مفتاحَ الإزاحةِ = 4، ننفذُ ما يأتي:

wii csy xshec

1. **نُطبّقُ المعادلةَ الآتيةَ لإيجادِ قيمةِ الإزاحةِ للنصِّ المشفَّرِ:** (22 = 4 – 26)، إذًا سيكونُ جدولُ التشفيرِ باستخدامِ الإزاحةِ 22 ، كما يأتي:

الحروف الأصلية	a	b	c	d	e	f	g	h	i	J	k	l	m	n	o	p	q	r	s	t	U	v	w	x	y	z
الحروف بعد الإزاحة	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v

2. **وبالاستعانةِ بجدولِ التشفيرِ يكونُ فكُّ التشفيرِ كما يأتي:**

الرسالة المشفرة	w	i	i		c	s	y		x	s	h	e	c
الرسالة الأصلية	s	e	e		y	o	u		t	o	d	a	y

إذًا، النصُّ الأصليُّ بعدَ فكِّ التشفيرِ هوَ :

see you today

نشاط عملي

أجرِّبُ فكَّ تشفيرِ الرسالةِ في المثالِ السابقِ بمِفتاحِ إزاحةٍ = 24. ماذا ألاحِظُ؟ أناقشُ الناتجَ معَ زملائي.

نشاط فردي

أحلِّلُ وأناقشُ

لديَّ النصُّ المشفرُ الآتي:

LW LV HDVB WR GHFUBSW

هلْ أستطيعُ اكتشـــافَ النصِّ الأصليِّ؟ ما مِفتاحُ التشفيرِ؟ كمْ منَ الوقتِ قضيتُ لفكِّ تشفيرِ النصِّ؟ ماذا أستنتجُ؟ أناقشُ إجاباتِ الأسئلةِ معَ الزملاءِ، ونتشاركُ في الأفكارِ والاقتراحاتِ.

نشاط عملي

أستخدمُ شيفرةَ قيصرَ بإزاحةٍ مقدارُها 6 لتشفيرِ الرسالةِ الأولى، وفكِّ تشفيرِ الرسالةِ الثانيةِ:

الرسالةُ الأولى: "Digital Skills are Your Key to The Future".

الرسالةُ الثانيةُ: "NUC EUA ZXKGZ UZNKX YGEY G RUZ GHUAZ EUAX YKRL"

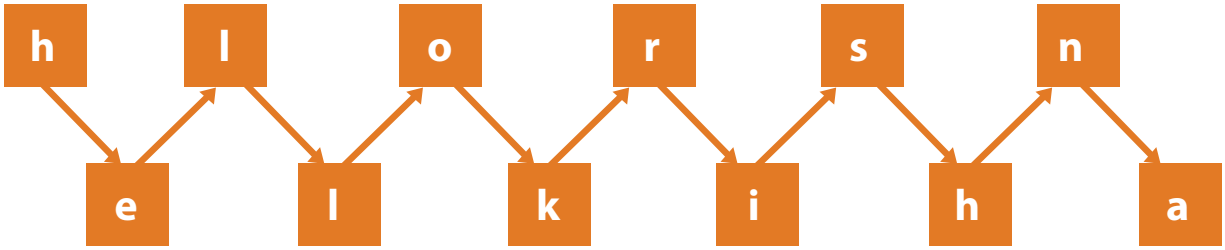
أقارنُ إجاباتي بإجاباتِ زملائي، ثمَّ أناقشُ ميزاتِ شيفرةِ قيصرَ وسلبياتِها بناءً على تجربتي.

تتميزُ شيفرةُ قيصرَ بعددٍ منَ المميزاتِ، فهيَ بسيطةٌ وسهلةُ التطبيقِ، ومناسبةٌ للمبتدئينَ، وتحتاجُ إلى معطياتٍ بسيطةٍ وهيَ قيمةُ الإزاحةِ، ويمكنُ تعديلُها بسهولةٍ لإنشاءِ حمايةٍ أقوى، كعملِ إزاحةٍ أكثرَ منْ مرةٍ.

أما سـلبياتُها، فهيَ خوارزميةٌ غيرُ آمنةٍ ضدَّ طرقِ فكِّ التشفيرِ الحديثةِ، ومحدودةُ الخياراتِ منْ قيمِ الإزاحةِ المحتملةِ وهيَ (26) قيمةٌ فقطْ؛ مما يجعلُ عمليةَ العثورِ على قيمةِ الإزاحةِ الصحيحِ سهلةً للغايةِ، وبذلكَ تكونُ النصوصُ عرضةً للاختراقِ بسـهولةٍ، ثمَّ إنَّها غيرُ مناسـبةٍ لتشفيرِ النصوصِ الطويلةِ.

شيفرةُ تبديلِ سياجِ السكةِ الحديديّةِ (Rail Fence Transposition Cipher):

وتُسمّى أيضًا شـيفرةَ الخطِّ المتعرجِ (Zig Zag Cipher)، وهيَ منْ خوارزمياتِ التشفيرِ بالإبدالِ، وتعدُّ تقنيةُ تشـفيرٍ بسيطةً، تعتمدُ على تبديلِ مواضعِ الحروفِ لإنتاجِ النصِّ المشفرِ بناءً على مفتاحِ تشفيرٍ يتعلقُ بعددِ أسطرِ التشفيرِ. ونبينُ خطواتِها عنْ طريقِ المثالِ الآتي:



مثال (3)

لتشفيرِ الرسالةِ الآتيةِ بعددِ أسطرٍ يساوي اثنينِ، نطبقُ الخطواتِ الموضحةَ لاحقًا:

nothing is as it seems

1. مَلْءُ رمزِ Ø مكانَ الفراغِ بينَ الكلماتِ في النصِّ، سيكونُ ناتجُ النصِّ كما يأتي:

nothingØisØasØitØseems

2. كتابةُ الرسالةِ الأصليةِ في سطرينِ (لأنَّ مِفتاحَ التشفيرِ سطرانِ) بطريقةِ الخطِّ المتعرِّجِ Zig Zag كما يأتي:

n		t		i		g		i		Ø		s		i		Ø		e		m	
	o		h		n		Ø		s		a		Ø		t		s		e		S

3. استخراجُ النصِّ المُشفّرِ بكتابةِ الحروفِ التي نتجتْ في الصفِّ الأولِ متتابعةً، ثمَّ الحروفِ التي نتجتْ في الصفِّ الثاني متتابعةً، فتصبحُ الرسالةُ المشفرةُ كما يأتي:

ntigiØsiØemohnØsaØtses

4. وبإزالةِ رمزِ الفراغِ الموجودِ في الاعلى Ø، تنتجُ الرسالةُ المشفرةُ الآتية:

ntigi si emohn sa tses

نشاط عملي

للتأكدِ منْ أنَّني قمتُ بعمليةِ التشفيرِ بالصورةِ الصحيحةِ، أستعينُ بالموقعِ الآتي.

عنْ طريقِ الرابطِ: https://cryptii.com/pipes/rail-fence-cipher أوْ عبرَ مسحِ رمزِ الاستجابةِ السريعِ المجاورِ الذي يقومُ بعمليةِ التشفيرِ ويعطيني الإجابةَ مباشرةً. أتأكدُ منْ إدخالِ عددِ الأسطرِ في مربعِ (Key).

نشاط عملي

أستخدمُ شيفرةَ تبديلِ سياجِ السكةِ الحديديةِ لتشفيرِ النصِّ الآتي بمِفتاحِ تشفيرٍ يساوي سطرينِ، ثمَّ أتأكدُ منْ إجابتي باستخدامِ الموقعِ الإلكترونيِّ:

https://cryptii.com/pipes/rail-fence-cipher.

"Believe in your Self"

أقارنُ إجابَتي بإجاباتِ زملائي.

لفكِّ تشفيرِ نصٍّ تمَّ تشفيرُهُ باستخدامِ شيفرةِ تبديلِ سياجِ السكةِ، نطبقُ الخطواتِ المبيَّنةَ في المثالِ (4):

مثال (4)

سنفكُّ تشفيرَ النصِّ الآتي، علمًا أنَّ مفتاحَ التشفيرِ يساوي سطرينِ:

IWL UCS HSYA ILSCESTI ER

1. ملْءُ الفراغاتِ بالرمزِ Ø فيصبحُ النصُّ:

IWLØUCSØHSYAØILSCESTIØER

2. عَدُّ حروفِ النصِّ المشفرِ (معَ الفراغاتِ) وهوَ في هذا المثالِ = 24 .

3. رسمُ جدولٍ مكوّنٍ منْ سطرينِ و24 عمودًا، ثمَّ نملأُ حروفَ النصِّ المشفرِ بالترتيبِ في الصفِّ الأولِ أفقيًّا، معَ تركِ مسافةٍ بينَ الحرفِ والآخرِ. ونكملُ ما تبقّى في الصفِّ الثاني.

كما هوَ مبيَّنٌ في الجدولِ الآتي:

I		W		L		Ø		U		C		S		Ø		H		S		Y		A	
	Ø		I		L		S		C		E		S		T		I		Ø		E		R

4. نقرأُ النصَّ بشكلِ الخطِّ المتعرِّجِ (Zig Zag) كما يظهرُ في الجدولِ الآتي:

I		W		L		Ø		U		C		S		Ø		H		S		Y		A	
	Ø		I		L		S		C		E		S		T		I		Ø		E		R

5. كتابةُ نصِّ الرسالةِ الأصليِّ، ثمَّ إزالةُ رمزِ الفراغِ (Ø) بينَ الحروفِ:

IØWILLØSUCCESSØTHISØYEAR

I WILL SUCCESS THIS YEAR

نشاط عملي

أستخدمُ شيفرةَ تبديلِ سياجِ السكةِ الحديديةِ Rail Fence Transposition Cipher)) لتشفيرِ النصِّ الآتي، علمًا بأنَّ مفتاحَ التشفيرِ يساوي سطرينِ.

BETTER LATE THAN NEVER

أتأكَّدُ منْ إجابتي باستخدامِ موقعِ التشفيرِ، وأقارنُها بإجاباتِ الزملاءِ:

https://cryptii.com/pipes/rail-fence-cipher

إثراء

ماذا لوْ كانَ مفتاحُ التشفيرِ يساوي ثلاثةَ أسطرٍ؟

سنتَّبعُ الإجراءاتِ نفسَها، ولكنْ بإنشاءِ جدولٍ يحتوي على ثلاثةِ أسطرٍ، كما هوَ مبيَّنٌ في الخطواتِ الآتيةِ:

النصُّ الأصليُّ: I think therefore I am

نضعُ رمزَ الفراغِ (ø)بينَ حروفِ النصِّ:

iøthinkøthereforeøIøam

I				i				t				e				e				A		
	ø		h		n		ø		h		r		f		r		ø		ø		m	
		t				k				e				o				i				

منْ الجدولِ الناتجُ، نكتبُ النصَّ المشفرَ بالبدءِ بحروفِ السطرِ الأولِ بالترتيبِ، ثمَّ السطرِ الثاني، ثمَّ السطرِ الثالثِ؛ فينتجُ لدينا النصُّ المشفرُ الآتي:

iiteeaøhnøhrfrøømtkeoi

وبإزالةِ رمزِ الفراغِ، فإنَّ النصَّ المشفرَ هوَ:

iiteea hn hrfr mtkeoi

للتأكدِ منْ صحةِ الحلِّ، أستخدمُ موقعَ التشفيرِ الآتي::

https://crypto.interactive-maths.com/rail-fence-cipher.html

نشاط عملي

قمْ بتشفيرِ النصِّ في المثالِ السابقِ بمفتاحِ تشفيرٍ: 4 أسطرٍ، وقمْ بالتحققِ منْ صحةِ تشفيرِكَ بالدخولِ إلى موقعِ: https: / /crypto.interactive-maths.com /rail-fence-cipher.html

- **حمايةُ الخصوصيةِ**: أستخدمُ التشـــفيرَ لحمايةِ البياناتِ الحساسةِ، مثلَ المعلوماتِ الشخصيةِ والماليةِ، ســـواءٌ عندَ تخزينِها أوْ نقلِها عبرَ الإنترنت. وأســـتخدمُ كلماتِ مرورٍ قويةً ومعقدةً، وأشـــفرُها عندَ تخزينِها؛ لضمانِ عدمِ الوصولِ غيرِ المصرحِ بهِ إلى الحســـاباتِ والمعلوماتِ الشخصيةِ.
- **الوعيُ بالمخاطرِ الأمنيةِ**: يجبُ أنْ أفهمَ أهميةَ التشفيرِ في حمايةِ بياناتِي منَ الاختراقِ والتجسسِ، وأنْ أعرفَ بأنَّ البياناتِ غيرَ المشفرةِ معرضةٌ للخطرِ عندَ نقلِها عبرَ الإنترنت.
- **احترامُ قوانينِ حمايـــةِ البياناتِ**: يجبُ أنْ ألتزمَ بالقوانينِ المحليـــةِ والدوليةِ المتعلقةِ بحمايةِ البياناتِ والخصوصيةِ، مثلَ اللائحةِ العامةِ لحمايةِ البياناتِ (GDPR) في الاتحادِ الأوروبيِّ.
- **التثقيفُ والتوعيةُ**: أشـــجعُ الأصدقاءَ والعائلةَ والزملاءَ على استخدامِ التشفيرِ وحمايةِ بياناتِهمْ بشكلٍ صحيحٍ، وأشارِكُ في برامجِ التوعيةِ والتدريبِ حولَ أهميةِ التشفيرِ وحمايةِ البياناتِ عبرَ الإنترنت.
- **الإسهامُ في مجتمعِ الأمانِ الرقميِّ**: أستخدمُ أدواتِ وبرامجَ التشفيرِ مفتوحةَ المصدرِ التي يمكنُ فحصُها منْ قبلِ الخبيرينَ؛ لضمانِ عدمِ وجودِ ثغراتٍ، وعندَ اكتشافِ ثغراتٍ أمنيةٍ أوْ ممارساتٍ غيرِ آمنةٍ، من الضروريِّ الإبلاغُ عنها للمؤسســـاتِ أوِ السلطاتِ المختصةِ للمساعدةِ في حمايةِ المجتمعِ الرقميِّ.

المشروعُ: حملةٌ إعلاميةٌ توعويةٌ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ/ مهمة 5

أتعاونُ معَ زملائِي لإنتاجِ المهمةِ الرابعةِ في الموادِّ التوعويةِ التي تتمحورُ حولَ إنتاجِ المطويةِ الإلكترونيةِ التفاعليةِ "مغامراتُ التشفيرِ: رحلتُكَ في أمانِ البياناتِ" باستخدامِ أداة (Canva)، لمشاركتِها في حملةٍ توعويةٍ حولَ أفضلِ ممارساتِ الأمنِ السيبرانيِّ، عبرَ اتباعِ الخطواتِ الآتيةِ:

التخطيطُ والتصميمُ:

- **اختيارُ العنوانِ والصورةِ للغلافِ**: تأكدْ أنَّ الصورةَ ترمزُ بوضوحٍ للتشفيرِ، وأنَّ العنوانَ جذابٌ وملفتٌ.
- **تحديدُ محتوى الصفحاتِ**: قسِّمِ المحتوى بينَ الصفحاتِ كما يأتي:
  - صفحةٌ لتعريفِ التشفيرِ وطرقِهِ وتصنيفاتِهِ.
  - **صفحاتٌ تطبيقيةٌ**: تحدياتٌ وألغازٌ، مثلُ شيفرةِ قيصرَ، وشيفرةِ تبديلِ سياجِ السكةِ الحديديةِ، معَ توفيرِ أمثلةٍ توضيحيةٍ.
  - صفحةٌ تحتوي على روابطَ لأدواتِ التشفيرِ، وفكِّ التشفيرِ.

إنشاءُ المحتوى:

- **كتابةُ النصوصِ**: صياغةُ نصوصٍ مختصرةٍ وواضحةٍ تشرحُ المفاهيمَ الأساسيةَ وتعطي تعليماتٍ للتطبيقِ.
- **تصميمُ الرسومِ البيانيةِ والمحاكاةِ**: استخدمْ أدواتٍ تفاعليةً لمحاكاةِ التشفيرِ أوْ توفيرِ ألغازٍ.
- **إضافةُ الروابطِ**: تأكدَ أنَّ الروابطَ صحيحةٌ وتقودُ إلى مواقعَ آمنةٍ ومفيدةٍ.

التصميمُ الجرافيكيُّ:

- **اختيارُ الألوانِ والخطوطِ**: استخدمْ تصميمًا جذابًا يتناسبُ معَ قِيَمِ التشفيرِ، معَ مراعاةِ القراءةِ السهلةِ والجاذبيةِ البصريةِ.
- **تنسيقُ الصفحاتِ**: رتِّبِ المعلوماتِ بشكلٍ منطقيٍّ وتسلسليٍّ يسهُلُ تتبُّعُهُ.

معاييرُ التقييمِ:

- **الشموليةُ والوضوحُ**: تأكدَ أنَّ المطويةَ تغطي كلَّ النقاطِ الرئيسةِ المطلوبةِ بدقةٍ وبلغةٍ واضحةٍ.
- **جودةُ التصميمِ**: قيِّمْ جاذبيةَ التصميمِ منْ حيثُ الألوانُ، والتنسيقُ، واستخدامُ الخطوطِ.
- **دقةُ الروابطِ وفعاليتُها**: تحققْ منْ صحةِ الروابطِ، وأنَّها تعملُ بشكلٍ صحيحٍ وآمنٍ.
- **الترتيبُ والتنظيمُ**: تأكدْ أنَّ المعلوماتِ مقدمةٌ بتسلسلٍ منطقيٍّ يسهِّلُ القراءةَ والفهمَ.

مشروع

أقيّمُ تعلُّمي

المعرفةُ: أستخدمُ ما تعلمتُهُ منْ معارفَ في هذا الدرسِ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: ما المعاييرُ التي تَّصنفُ على أساسِها خوارزمياتُ التشفيرِ؟

.....

السؤالُ الثاني: ما الفرقُ بينَ التشفيرِ بالتعويضِ والتشفيرِ بالإبدالِ معَ إعطاءِ مثالٍ على كلٍّ منهما؟.

.....

.....

السؤالُ الثالثُ: أقارنُ بينَ تشفيرِ الكتلِ وتشفيرِ التدفقِ منْ حيثُ:

- الأمانُ.

.....

- آليةُ التشفيرِ.

.....

- الوقتُ المستهلَكُ.

.....

- البساطةُ.

.....

السؤالُ الرابعُ: أشفرُ النصَّ " My School is my second home "، مستخدمًا الشيفراتِ الآتيةَ:

شيفرةُ قيصرَ بقيمةِ إزاحةٍ = 6.

شيفرةُ تبديلِ سياجِ السكةِ الحديديةِ بمفتاحِ التشفيرِ = 4 أسطرٍ.

.....

.....

السؤالُ الخامسُ: أفكُّ تشفيرَ النصِّ الآتي مستخدمًا شيفرةَ قيصرَ، علمًا بأنَّ قيمةَ الإزاحةِ = 3.

L OLNH ILQH DUWV

.....

.....

المهاراتُ: أستخدمُ مهاراتِ البحثِ الرَّقْميِّ، والتفكيرَ الناقدَ والتواصلَ الرَّقْميَّ، وأجيبُ عنِ الأسئلةِ الآتيةِ:

الســـؤالُ الأولُ: أقارنُ بينَ طرقِ التشفيرِ المختلفةِ التي تعلَّمتُها بإنشـــاءِ إنفوجرافيك Infogrphic باستخدامِ برمجيةِ Canva، ومشاركتِهِ على الحائطِ التفاعليِّ بادلتْ Padlet الخاصِّ بالصفِّ.

.....

.....

السؤالُ الثاني: أبحثُ في طرقِ تشفيرٍ أخرى غيرِ التي تعرفتُ إليها في الدرسِ وأكتبُ تقريرًا عنها.

.....

.....

الســـؤالُ الثالثُ: هلْ يعدُّ التشفيرُ وسيلةً قويةً لحمايةِ البياناتِ الحساسةِ؟ هلْ يكفي التشفيرُ لحمايةِ البياناتِ؟ هلْ توجدُ طرقٌ أخرى للحمايةِ؟ أكتبُ أفكاري ومقترحاتي.

.....

.....

القِيَمُ والاتجاهاتُ

أتعاونُ معَ الزملاءِ لتصميمِ بوسترٍ لنشرِ التوعيةِ والتثقيفِ بينَ الأهلِ والزملاءِ في المدرسةِ عنْ أهميةِ حمايةِ البياناتِ الشخصيةِ، ودورِ التشفيرِ في حمايتِها، معَ تقديمِ مقترحاتٍ حولَ طرقِ تشفيرٍ بسيطةٍ يمكنُ تطبيقُها. أنشرُ البوسترَ في مواقعِ التواصلِ الاجتماعيِّ للمدرسةِ.

ملخصُ الوحدةِ

تعرَّفْنا في هذهِ الوحدةِ إلى أهميةِ حمايةِ البياناتِ والطرقِ المتبعةِ لحمايةِ البياناتِ وخاصةً كلمةَ السرِّ، وتعرَّفْنا أيضًا إلى مشكلاتِ الأمنِ السيبرانيِّ، وتوصياتِ الأمنِ السيبرانيِّ، وطبَّقْنا بعضَ الوسائلِ الماديةِ والرقميةِ لتحقيقِ توصياتِ الأمنِ السيبرانيِّ، وتعرَّفْنا أيضًا إلى توصياتِ الأمنِ السيبرانيِّ، وأصبحَ بإمكانِنا مقارنةُ وسائلِ حمايةِ البياناتِ تبعًا لمقاييسَ محددةٍ مثلِ الفعاليةِ والجدوى والتأثيراتِ الأخلاقيةِ، وطبَّقْنا كذلكَ طرقًا مختلفةً منَ التشفيرِ.

في ما يأتي أبرزُ الجوانبِ الّتي تناولتْها الوَحدةُ:

- تعدُّ حمايةُ البياناتِ منِ الموضوعاتِ الحيويةِ في عالمِ التكنولوجيا الحديثةِ؛ حيثُ تتنوعُ طرقُ حمايةِ البياناتِ لتشملَ استخدامَ كلماتِ المرورِ القويةِ، والتشفيرَ، والجدرانَ الناريةَ، وبرامجَ مكافحةِ الفيروساتِ، والنسخَ الاحتياطيَّ الدوريَّ للبياناتِ، والتحكمَ في الوصولِ والصلاحياتِ. ويعتمدُ اختيارُ الطريقةِ الأنسبِ لحمايةِ البياناتِ على طبيعتِها.
- تعدُّ كلماتُ السرِّ إحدى أهمِّ وسائلِ حمايةِ البياناتِ، فهيَ رموزٌ سريةٌ تستخدمُ للتحققِ منْ هُويةِ المستخدمينَ وتقييدِ الوصولِ إلى البياناتِ. تعدُّ كلماتُ السرِّ القويةُ ضروريةً لمنعِ الوصولِ غيرِ المصرحِ بهِ وحمايةِ البياناتِ الشخصيةِ، ويجبُ أنْ تكونَ طويلةً ومعقدةً، وتشملَ حروفًا كبيرةً وصغيرةً وأرقامًا ورموزًا خاصةً.
- لحمايةِ البياناتِ منْ مشكلاتِ الأمنِ السيبرانيِّ، يجبُ تصنيفُ وسائلِ الحمايةِ إلى وسائلَ ماديةٍ، مثلَ قفلِ الأجهزةِ، ومراقبةِ الدخولِ، والتخزينِ الآمنِ للأجهزةِ، ووسائلَ رقميةٍ تشملُ التشفيرَ، والجدرانَ الناريةَ، وبرامجَ مكافحةِ الفيروساتِ. وتشملُ مشكلاتُ الأمنِ السيبرانيِّ السرقةَ الرقميةَ والقرصنةَ وانتهاكاتِ الخصوصيةِ، وتتطلبُ حمايةُ البياناتِ الشخصيةِ تطبيقَ ممارساتِ أمانٍ قويةٍ. وقدْ يتطلبُ تطبيقُ توصياتِ الأمنِ السيبرانيِّ المختلفةِ بعضَ التنازلاتِ، مثلَ زيادةِ التعقيدِ في الوصولِ إلى البياناتِ والتكاليفِ الإضافيةِ.
- الهجماتُ الإلكترونيةُ هيَ محاولاتٌ لاختراقِ الأنظمةِ والحصولِ على بياناتٍ منْ دونِ إذنٍ، وتشملُ الاعتداءَ الإلكترونيَّ، والتجسسَ، والسرقةَ، وتدميرَ البياناتِ. إنَّ مناقشةَ قضايا واقعيةٍ تتعلقُ بالأمنِ السيبرانيِّ، مثلَ حوادثِ اختراقِ البياناتِ في الشركاتِ الكبيرةِ، وتسريبِ المعلوماتِ الشخصيةِ، وانتشارِ البرمجياتِ الخبيثةِ تظهرُ أهميةُ هذا الموضوعِ. وتعتمدُ حمايةُ

المعلوماتِ على تكاملِ الوسائلِ الماديةِ والرقميةِ.

- تعدُّ المعلوماتُ المتوافرةُ على الشبكةِ مهمةً، وتكمنُ قيمتُها في توفيرِها للمعرفةِ التي يحتاجُها صناعُ القرارِ لاتخاذِ قراراتِهمْ المهمةِ. إنَّ ممارسةَ الأفرادِ للأنشطةِ اليوميةِ الرقميةِ على شبكةِ الإنترنتْ، يتركُ مجموعةً كبيرةً منْ البياناتِ الخاصةِ بالأفرادِ مخزنةً على الشبكةِ؛ مما يتيحُ لمجرمي الإنترنتْ سرقتَها واختراقَها واستغلالَها لذا؛ يجبُ أنْ نعملَ على حمايتِها.
- يوجدُ عديدٌ منْ التطبيقاتِ والمواقعِ بعيدةٌ عنْ ميزةِ الوصولِ للخدمةِ، (Accessibility) وهيَ قدرةُ الجميعِ على استخدامِ منتجٍ أوْ خدمةٍ، أوْ إتاحةُ الوصولِ للجميعِ بمنْ فيهمْ كبارُ السنِّ وذوي الإعاقةِ؛ لذا يجبُ ضمانُ حصولِ الجميعِ بمنْ فيهمْ كبارُ السنِّ وذوي الإعاقةِ على فرصٍ متساويةٍ للوصولِ إلى التطبيقاتِ والتقنياتِ عبرَ شبكةِ الإنترنتْ، وهناكَ عديدٌ منْ ميزاتِ إمكانيةِ الوصولِ، منها (قارئُ الشاشةِ، وتباينُ الألوانِ).
- **يوجدُ عديدٌ منْ وسائلِ الحمايةِ التي تحدُّ منْ مشكلاتِ مشاركةِ البياناتِ، منها:** تشفيرُ البياناتِ (Encryption)، والنسخُ الاحتياطيُّ (Backup and Recovery)، وضبطُ صلاحياتِ الوصولِ (Access Control)، والمصادقةُ (Authentication)، والتوقيعُ الرقميُّ، وسياساتُ الخصوصيةِ (Privacy Policies). وتختلفُ هذهِ الطرقُ منْ حيثُ فعاليتُها والجدوى منْ استخدامِها وتأثيرُها الأخلاقيُّ.
- التشفيرُ هوَ عمليةُ تحويلِ النصِّ الأصليِّ إلى نصٍّ غيرِ مفهومٍ إلا للشخصِ المرَسلِ والشخصِ المستقبلِ للرسالةِ؛ وذلكَ بهدفِ إخفاءِ معلوماتِ الرسالةِ الأصليةِ، وجعلِها غيرَ مقروءةٍ أوْ مفهومةٍ للمستلمينَ غيرِ المقصودينَ. وهناكَ عديدٌ منْ خوارزمياتِ التشفيرِ التي تُصنفُ بحسبِ ثلاثةِ معاييرَ.
- **المعيارِ الأولِ:** هوَ نوعُ عمليةِ التشفيرِ المستخدمةِ مثلَ
  - خوارزمياتِ التعويضِ (Substitution) كخوارزميةِ قيصرَ (Caesar Cipher).
  - خوارزمياتِ الإبدالِ (Transposition)، كخوارزميةِ تبديلِ سياجِ السكةِ الحديديةِ (Rail Fence transposition Cipher).
  - خوارزميةِ المنتجِ (Product) والتي تجمعُ بينَ تحويلينِ أوْ أكثرَ لتشفيرِ البياناتِ.

- **المعيارُ الثاني**: لتصنيفِ خوارزمياتِ التشفيرِ فهوَ مفتاحُ التشفيرِ المستخدمُ مثلَ
  - خوارزميةِ التشـــفيرِ المتماثلِ (Symmetric encryption) أوْ تســـمى أحيانًا بتشفيرِ المفتاحِ الخاصِّ (Private Key Cryptography) ويَستخدمُ المرســـلُ والمستقبلُ فيها المفتاحُ نفسَهُ للتشفيرِ وفكِّ التشفيرِ.
  - خوارزميـــةِ التشـــفيرِ غيـــرُ المتماثـــلِ، أوْ تســـمى أحيانًـــا تشـــفيرَ المفتـــاحِ العامِّ (Public Key Cryptography) حيثُ يُستخدمُ مفتاحانِ؛ واحدٌ للتشفيرِ والثاني لفكِّ التشفيرِ.
- **المعيارُ الثالثُ**: بحســـبِ طريقةِ معالجةِ النصِّ الأصليِّ، مثلَ؛ تشـــفيرِ الكتلِ (Block) وتشفيرِ التدفقِ (Stream Cipher).

أسئلةُ الوحدةِ

السؤالُ الأولُ: أعرِّف كلًا منَ المصطلحاتَ الآتيةَ:

- المصادقةَ(Authentication).

.....

- التشفيرُ (Encryption) .

.....

- ميزةَ الوصولِ للخدمةِ (Accessibility).

.....

السؤالُ الثاني: أقارنُ بينَ كلِّ مصطلحينِ في ما يأتي:

- تشفيرُ الكُتلِ وتشفيرُ التدفُّقِ.

.....

.....

- التشفيرُ المتماثلُ والتشفيرُ غيرُ المتماثلِ.
- Wiping و Deleting.

.....

.....

السؤالُ الثالثُ: أعدِّد الطرقَ المستخدمةَ برمجيًّا لحمايةِ البياناتِ معَ ذكرِ أمثلةٍ على كلٍّ منها.

.....

.....

.....

السؤالُ الرابعُ:

1. أيُّ الطرقِ هيَ الأنسبُ لحمايةِ المعلوماتِ الماليةِ الحساسةِ؟ أفسّرُ إجابَتي.

.....

.....

.....

2. أبينُ كيفَ يمكنُ حمايةُ البياناتِ الشخصيةِ بطريقةٍ فعّالةٍ معَ تقديمِ مقترحاتٍ.

.....

.....

.....

السؤال الخامس: أضع دائرة حول رمز الإجابة الصحيحة في كلّ مما يأتي:

1- أحد الآتية يعدُّ من العناصر الرئيسة لأمن المعلومات:

أ. الاستجابة للحوادث ب. التشفير ج. النسخ الاحتياطي

2- الركائز الثلاث لأمن المعلومات هي:

أ. السرِّية، التوافر، النزاهة ب- السرِّية، الخصوصية، التوافر ج- النزاهة، السرِّية، الخصوصية

3- من أشهر الثغرات الأمنية التي تصيب الأجهزة:

أ. Meltdown ب. SSL /TLS ج. Maleware

4- من الوسائل المادّية المستخدمة للحماية من تهديدات الأمن السيبراني:

أ. جدران الحماية ب. ضوابط الوصول الفيزيائي ج. البرامج المضادة للفيروسات

5- الخوارزمياتُ التي تعتمد على تغيير حروف الرسالة بحروفٍ أخرى مثل شيفرة قيصر (Caesar Cipher) تعدّ من خوارزميات:

أ. خوارزميات التعويض ب. خوارزميات الإبدال ج. خوارزميات المُنتج

السؤالُ السادس:

I WILL STUDY WELL THIS YEAR

أشفِّر النصَّ أعلاهُ باستخدامِ شيفرةِ قيصرَ ومفتاحِ إزاحةٍ بقيمةِ 6.

أشفِّرُ النصَّ أعلاهُ باستخدامِ شيفرةِ تبديلِ سياجِ السكةِ الحديديةِ (Rail Fence Transposition Cipher) ومفتاحِ عددِ أسطرٍ =2.

أقارنُ بينَ الطريقتيْنِ في التشفيرِ، أيُّهُما أكثرُ تعقيدًا وأكثرُ صعوبةً في الاختراقِ؟ أُبرّرُ إجابتي؟

.....

.....

.....

.....

.....

.....

.....

.....

السؤالُ السابع: أفكُّ شيفرةَ النصِّ الآتي:

Iwl td ye euiy ilsuycbrscrt

باستخدامِ شيفرةِ تبديلِ سياجِ السكةِ الحديديةِ (Rail Fence Transposition Cipher) ومفتاحِ عددِ أسطرٍ=2 ..

.....

.....

.....

.....

.....

تقويمٌ ذاتيٌّ (Self-Checklist)

بعدَ دراستي هذهِ الوحدةَ، اقرأُ الفقراتِ الواردةَ في الجدولِ الآتي، ثمَّ أضعُ إشارةَ (✔) في العمودِ المناسبِ:

مؤشراتُ الأداءِ	نعمْ	لا	لستُ مُتأكِّدًا
أوضحَ مفهومَ حمايةِ البياناتِ.	○	○	○
أميزُ بينَ أمنِ البياناتِ والمعلوماتِ والأمنِ السيبرانيِّ.	○	○	○
أبينَ عناصرَ أمنِ المعلوماتِ.	○	○	○
أوضحَ ركائزَ أمنِ المعلوماتِ.	○	○	○
أشرحُ سببَ استخدامِ كلماتِ السرِّ لحمايةِ المعلوماتِ.	○	○	○
أصنفَ وسائلَ الحمايةِ منْ مشكلاتِ الأمنِ السيبرانيِّ إلى وسائلَ ماديةٍ ووسائلَ رقميةٍ.	○	○	○
أوضحَ مشكلاتِ الأمنِ السيبرانيِّ وحمايةِ البياناتِ الشخصيةِ.	○	○	○
أبينُ مفهومَ الهجماتِ الإلكترونيةِ والاعتداءِ الإلكترونيِّ.	○	○	○
أناقشُ قضايا واقعيةً تتعلقُ بالأمنِ السيبرانيِّ.	○	○	○
أوضحَ كيفَ تقومُ وسائلُ الأمنِ الماديةُ والرقميةُ بحمايةِ المعلوماتِ.	○	○	○
أعددُ أمثلةً على الوسائلِ الماديةِ للحمايةِ والوسائلِ الرقميةِ للحمايةِ.	○	○	○

مؤشراتُ الأداءِ	نعمْ	لا	لستُ مُتأكِّدًا
أصفُ أهميةَ الخبراتِ السابقةِ في إنشاءِ توصياتِ الأمنِ السيبرانيِّ.	○	○	○
أصفُ العلاقةَ بينَ احتياجاتِ المستخدمِ وتعارضِها (أحيانًا) معَ توصياتِ الأمنِ السيبرانيِّ.	○	○	○
أوضحَ العلاقةَ بينَ ميزةِ الوصولِ للخدمةِ Accessibility وتوصياتِ الأمنِ السيبرانيِّ.	○	○	○
أوضحَ الطرقَ المستخدمةَ برمجيًا لحمايةِ البياناتِ.	○	○	○
أقيمُ وسائلَ حمايةِ البياناتِ من حيثُ فعاليتُها والجدوى من استخدامِها وتأثيرُها الأخلاقيُّ.	○	○	○
أعرفُ عمليةَ تشفيرِ البياناتِ وأبينُ أهميتِها لحمايةِ البياناتِ.	○	○	○
أصفُ الطرقِ البسيطةِ والمعقدةِ لتشفيرِ البياناتِ.	○	○	○
أطبقُ عملياتِ التشفيرِ وفكِّ التشفيرِ باستخدامِ طرقٍ ومستوياتِ صعوبةٍ مختلفةٍ.	○	○	○

تعليماتٌ للمراجعةِ والتحسينِ:

إذا اخترْتُ (لا) أوْ (لستُ مُتأكِّدًا) لأيٍّ منَ الفقراتِ السابقةِ، فأتَّبعُ الخطواتِ الآتيةَ لتجنُّبِ ذلكَ:

- أُراجِعُ المادةَ الدراسيةَ؛ بأنْ أُعيدَ قراءةَ المحتوى المُتعلِّقِ بالمعيارِ.
- أطلبُ المساعدةَ؛ بأنْ أُناقِشَ مُعلِّمي/ مُعلِّمتي أوْ زملائي/ زميلاتي في ما تعذَّرَ عليَّ فهمُهُ.
- أستخدِمُ مراجعَ إضافيةٍ؛ بأنْ أبحثَ عنْ مراجعَ أُخرى مثلِ الكتبِ، أوْ أستعينَ بالمواقعِ الإلكترونيةِ الموثوقةِ التي تُقدِّمُ شرحًا وافيًا للموضوعاتِ التي أجدُ صعوبةً في فهمِها.

تأمُّلاتٌ ذاتيةٌ

عزيزي الطالبَ/ عزيزتي الطالبةَ:

التأمُّلاتُ الذاتيةُ هيَ فرصةٌ لتقييمِ عمليةِ التعلُّمِ، وفهمِ التحدِّياتِ، وتطويرِ استراتيجياتٍ لتحسينِ عمليةِ التعلُّمِ مستقبلًا. أملأُ الفراغَ في ما يأتي بالأفكارِ والتأمُّلاتِ الشخصيةِ التي يُمكِنُ بها تحقيقُ أفضلِ استفادةٍ منَ التجربةِ التعليميةِ:

تعلَّمْتُ في هذهِ الوحدةِ:

يُمكِنُني أنْ أُطبِّقَ ما تعلَّمْتُهُ في:

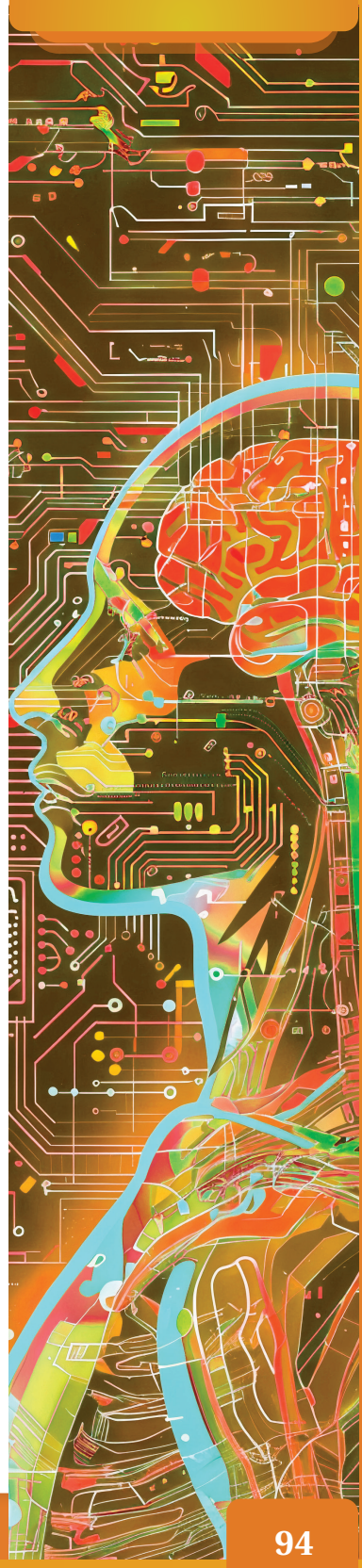
الصعوباتُ التي واجهْتُها أثناءَ عمليةِ التعلُّمِ:

ذلَّلْتُ هذهِ الصعوباتِ عنْ طريقِ:

يُمكِنُني مستقبلًا تحسينُ:

الوحدة

الذكاءُ الاصطناعيُّ (Artificial Intelligence)



نظرةٌ عامّةٌ على الوَحْدةِ:

في هذهِ الوَحْدةِ، سأتعرفُ إلى مفهومِ الذكاءِ الاصطناعيِّ ومكوناتِهِ وخصائصِهِ. بالإضافةِ إلى كيفيةِ عملِ أنظمةِ الذكاءِ الاصطناعيِّ ومراحلِ تطوُّرِها، وسأتعلمُ كيفَ أُميِّزُ بينَ أنظمةِ الذكاءِ الاصطناعيِّ والأنظمةِ التقليديةِ، وأستكشفُ مجالاتِ استخدامِ الذكاءِ الاصطناعيِّ، وسأُجرِّبُ أيضًا بعضَ تطبيقاتِ الذكاءِ الاصطناعيِّ وأُحدِّدُ خصائصَها. وفي النهايةِ، سأبحثُ في التأثيراتِ الاجتماعيةِ للذكاءِ الاصطناعيِّ، وكيفَ يُؤثّرُ في حياتِنا اليوميةِ. بالإضافةِ إلى ذلكَ، سأتعرّفُ إلى الروبوتِ بوصفِهِ أحدَ تطبيقاتِ الذكاءِ الاصطناعيِّ بشكلٍ خاصٍّ، وإلى مكوناتِهِ، وأهميتِهِ، واستخداماتِهِ، وكيفيةِ بَرمجتِهِ في بيئةٍ افتراضيةٍ.

يُتوقّعُ مني معَ نهايةِ الوَحْدةِ أنْ أكونَ قادرًا على:

- تعريفِ الذكاءِ الاصطناعيِّ وتوضيحِ خصائصِهِ.
- التمييزِ بينَ أنظمةِ الذكاءِ الاصطناعيِّ والأنظمةِ التقليديةِ.
- توضيحِ أهميةِ الذكاءِ الاصطناعيِّ.
- توضيحِ مجالاتِ تطبيقِ الذكاءِ الاصطناعيِّ في النُّظمِ المعرفيةِ الأخرى.
- توضيحِ تطبيقاتِ الذكاءِ الاصطناعيِّ.
- استخدامِ إحدى أدواتِ الذكاءِ الاصطناعيِّ في تطبيقاتٍ واقعيةٍ.
- تمييزِ الآثارِ الاجتماعيةِ للذكاءِ الاصطناعيِّ.
- توضيحِ مكوناتِ نظامِ الروبوتِ وكيفيةِ عملِهِ.
- توضيحِ أهميةِ الروبوتِ وتمييزِ بعضِ استخداماتِهِ.
- برمجةِ الروبوتِ على الحركاتِ الأساسيةِ في بيئةٍ افتراضيةٍ.

منتجاتُ التعلّم (Learning products)

إنتاجُ سلسلةٍ منْ مقاطعِ الفيديو التعليميةِ (الرسومِ المتحركةِ) على شكلِ حلقاتٍ؛ حيثُ تتناولُ كلُّ حلقةٍ موضوعًا مُحدّدًا، باستخدامِ تطبيقاتِ الذكاءِ الاصطناعيِّ لاختيارِ الشخصياتِ، وتسجيلِ الأصواتِ، وتحريكِ المشاهدِ؛ لضمانِ تقديمِ محتوًى شائقٍ وجذّابٍ.

مشروع

أختارُ معَ أفرادِ مجموعتي أحدَ المشروعاتِ الآتيةِ لتنفيذِهِ في نهايةِ الوَحْدةِ

- **المشروعُ الأوّلُ**: تطويرُ تطبيقِ ذكاءٍ اصطناعيٍّ يساعدُ الطلبةَ في تحديدِ النظامِ التعليميِّ الأنسبِ لهمْ بينَ النظامِ الأكاديميِّ ونظامِ (BTEC)؛ وذلكَ باستخدامِ تطبيقِ (Mobile App)، الذي يدعمُ دمجَ أدواتِ الذكاءِ الاصطناعيِّ.
- **المشروعُ الثاني**: تطويرُ تطبيقِ ذكاءٍ اصطناعيٍّ مخصّصٍ لتلبيةِ احتياجاتٍ محددةٍ في مجالٍ معينٍ عنْ طريقِ استخدامِ تطبيقِ (Mobile App)، الذي يدعمُ دمجَ أدواتِ الذكاءِ الاصطناعيِّ.
- **المشروعُ الثالثُ**: برمجةُ لعبةٍ باستخدامِ برنامجِ (Scratch)، معَ تضمينِ أدواتِ الذكاءِ الاصطناعيِّ المتوافرةِ في البرنامجِ

المهاراتُ الرَّقْميةُ: البحثُ الرَّقْميُّ، التفكيرُ الحاسوبيُّ، التعاونُ الرَّقْميُّ، التواصلُ الرَّقْميُّ، حلُّ المشكلاتِ البرمجيةِ.

فهرسُ الوَحْدةِ

Virtual Robotics Simulator

Google Docs

Canva

Chrome Edge Firefox

الدرسُ الأوّلُ

مقدمةٌ في الذكاءِ الاصطناعيِّ
(Introduction to Artificial Intelligence)

الفكرةُ الرئيسةُ:

لتعرُّفُ إلى مفهومِ الذكاءِ الاصطناعيِّ ومكوناتِهِ، واستكشافِ خصائصِهِ، وَتتبعِ مراحلِ تطوّرِهِ.

المفاهيمُ والمصطلحاتُ:

الذكاءُ الاصطناعيُّ (Artificial Intelligence)،
معالجةُ اللغاتِ الطبيعيّةِ (Natural Language Processing)،
أتمتةُ المهامِّ البسيطةِ والمتكررةِ
(Automate Simple and Repetitive Tasks)،
استيعابُ البياناتِ (Data Ingestion)، محاكاةُ الإدراكِ البشريِّ
(Imitation of Human Cognition)، التخطيطُ (Planning)،
الإدراكُ (Perception)، المنطقُ واتخاذُ القرارِ
(Reasoning and Decision Making)،
حلُّ المشكلاتِ (Problems Solving).

نتاجاتُ التعلّمِ (Learning Outcomes)

- أُعرّفُ الذكاءَ الاصطناعيَّ، وأذكرُ أمثلةً على أنظمتِهِ.
- أُبينُ مكوناتِ نظامِ الذكاءِ الاصطناعيِّ.
- أشرحُ آليةَ عملِ نظامِ الذكاءِ الاصطناعيِّ.
- أُقارنُ بينَ أنظمةِ الذكاءِ الاصطناعيِّ والأنظمةِ التقليديةِ.
- أبينُ خصائصَ الذكاءِ الاصطناعيِّ.
- أُميّزُ أنظمةَ الذكاءِ الاصطناعيِّ.
- أُبينُ مراحلَ تطورِ الذكاءِ الاصطناعيِّ.
- أُوضحُ أهميةَ الذكاءِ الاصطناعيِّ.

منتجاتُ التعلّمِ
(Learning Products)

أُنشئُ لوحةً قصصيةً مفصّلةً، تشتملُ على تحديدِ الشخصياتِ، والحواراتِ المكتوبةِ والمسموعةِ، والخلفياتِ. بالإضافةِ إلى التسلسلِ البصريِّ للمشاهدِ، ويجبُ تحديدُ التطبيقِ الذي ستعملُ عليهِ اللوحاتُ، وستكونُ هذهِ اللوحةُ القصصيةُ المرجعَ الأساسيَّ خلالَ مرحلةِ إنتاجِ الفيديوهاتِ.

نشاط تمهيدي

بالاعتمادِ على ما تعلمتُهُ أوْ شـــاهدتُهُ أو قرأتُهُ، أُعطي أمثلةً على آلاتٍ ذكيّةٍ، وأُبينُ سببَ إطلاقِ هذهِ الصفةِ عليها، ثمَّ أدونُ ملاحظاتي وأُشاركُها معَ زملائي في الصفِّ.

أصبحَ للذكاءِ الاصطناعيِّ دورٌ أساســيٌّ في حياتِنا، وتطورَ اســتخدامُهُ تطورًا كبيرًا؛ فمنْ مُشغّلٍ لمحركاتِ البحــثِ، إلى مُقدمِ توصياتٍ بالمنتجاتِ، إلى تعرُّفِ الــكلامِ عنْ طريقِ أنظمةٍ خاصّةٍ وغيرِها منْ محاكاةٍ لطريقةِ تفكيرِ الإنسانِ وسلوكِهِ. في كثيرٍ منَ الأحيانِ سيكونُ الذكاءُ الاصطناعيُّ مرافقًا لرحلاتِنا منْ وِجهةٍ إلى أُخــرى عنْ طريقِ (GPS) وغيرِها منَ الخدماتِ الكثيرةِ. فما مفهومُ الذكاءِ الاصطناعيِّ؟ وما مكوناتُهُ وخصائصُهُ ومميزاتُهُ؟ وما مراحلُ تطورِهِ؟

الذكاءُ الاصطناعيُّ (Artificial Intelligence)

يُعدُّ الذكاءُ الاصطناعيُّ أحدَ فروعِ علومِ الحاسوبِ، ويُعرّفُ بأنّهُ القدرةُ على مُحاكاةِ أنشطةِ الذكاءِ البشــريِّ مثلَ: التعلّمِ والتنبؤِ والاستدلالِ والتنظيمِ الذاتيِّ والقدرةِ على حلِّ المشــكلاتِ واتخاذِ القراراتِ، باستخدامِ تِقْنيّاتٍ مشابهةٍ لقدرةِ الإنسانِ للتعرّفِ إلى الأشياءِ، والفهمِ والاستجابةِ والتطورِ.

ويُعــرّفُ نظامُ الذكاءِ الاصطناعيِّ بأنّهُ نظامٌ آلــيٌّ تمتْ برمجتُهُ للقيامِ بمجموعةٍ منَ الوظائفِ لتحقيقِ أهــدافٍ محددةٍ، وهوَ قادرٌ على توليدِ مخرجاتٍ مثلَ: تقديمِ التنبــؤاتِ أوِ التوصياتِ أوِ القــراراتِ عنْ طريقِ عملياتِ الرّبطِ والاســتنتاجِ، ولَهُ القدرةُ على تحسينِ ذاتِهِ اعتمادًا على البياناتِ التي يجمعُها، ويُمكنُ لمخرجاتِهِ التأثيرُ في البيئاتِ الحقيقيّةِ أوِ الافتراضيةِ.

نشاط فردي

أبحثُ وأشاركُ

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنْ تعريفاتٍ أُخرى لنظامِ الذكاءِ الاصطناعيِّ، وأشاركُ زملائي بما توصلتُ إليهِ علــى اللوحِ التفاعليِّ للصفِ (Padlet)، وأتصفحُ وأقرأُ مشــاركاتِ زملائي، وأُعقّبُ على أكثرِ تعريفيْنِ لفتا انتباهي، معَ تقديمِ ملاحظاتٍ بنّاءةٍ، تُوضّحُ لماذا أثارتْ تلكَ التعريفاتُ اهتمامي.

تختلفُ أهدافُ أنظمةِ الذكاءِ الاصطناعيِّ باختلافِ مجالاتِ استخدامِهِ، وبشكلٍ عامٍّ، يهدفُ الذكاءُ الاصطناعيُّ إلى:

- **أتمتةِ العملياتِ المُعقّدةِ**: عنْ طريقِ تطويرِ أنظمةٍ ذكيّةٍ، يمكنُها تنفيذُ مهامَّ تتطلبُ التفكيرَ أوِ اتخاذَ القراراتِ، مثلَ التشخيصِ الطبيِّ، والتعرّفِ إلى الصورِ، أوِ التفاعلِ معَ العملاءِ.
- **تحسينِ الكفاءةِ**: عنْ طريقِ زيادةِ الإنتاجيةِ، وتقليلِ الأخطاءِ البشريةِ باستخدامِ الذكاءِ الاصطناعيِّ في الصناعاتِ المختلفةِ.
- **توسيعِ القدراتِ البشريةِ**: بدعمِ قدراتِ البشرِ وتعزيزِها في مجالاتٍ، مثلَ الطبِّ، والتعليمِ، والبحوثِ العلميةِ.
- **حلِّ المشكلاتِ المعقّدةِ**: بتوفيرِ أدواتٍ لتحليلِ البياناتِ الضخمةِ، والتنبؤِ بالاتجاهاتِ المستقبليةِ، وتحليلِ الأنماطِ التي قدْ تكونُ صعبةً أوْ يستحيلُ على البشرِ التعاملُ معَها، وإيجادِ حلولٍ للمشكلاتِ التي يصعبُ حلُّها بسببِ تعقيدِها أوْ حجمِها الكبيرِ، مثلَ تحسينِ أنظمةِ النقلِ أوْ محاكاةِ النُّظمِ البيئيةِ.
- **ابتكارِ حلولٍ جديدةٍ**: بتطويرِ تِقْنيّاتٍ جديدةٍ لمشكلاتٍ قديمةٍ عنْ طريقِ التفكيرِ المبتكرِ القائمِ على الذكاءِ الاصطناعيِّ

نشاط جماعي

أفكرُ معَ زملائي في المجموعةِ في مشكلةٍ معاصرةٍ (سواءٌ أكانتْ اجتماعيةً، أوْ اقتصاديةً، أوْ تعليميةً)، ثمَّ نناقشُ معًا كيفَ يمكنُ للذكاءِ الاصطناعيِّ الإسهامُ في حلِّ هذهِ المشكلةِ. بعدَ ذلكَ، نقومُ بتلخيصِ المشكلةِ والحلولِ المقترحةِ، معَ توضيحِ دورِ الذكاءِ الاصطناعيِّ في معالجةِ هذهِ التحدياتِ، ثمَّ نعرضُ نتائجَ مناقشتِنا ونشارِكُها معَ المجموعاتِ الأخرى، ونتبادلُ النقاشَ في وجهاتِ النّظرِ المختلفةِ، بشأنِ كيفيةِ الاستفادةِ مِنَ الذكاءِ الاصطناعيِّ في هذهِ المجالاتِ.

مكوناتُ أنظمةِ الذكاءِ الاصطناعيِّ

يتكونُ نظامُ الذكاءِ الاصطناعيِّ منْ عناصرَ أساسيةٍ يتكاملُ بعضُها معَ بعضٍ لتشكّلَ نظامًا ذكيًّا قادرًا على محاكاةِ ذكاءِ الإنسانِ. وفي ما يأتي عرضٌ لأهمِّ هذهِ المكوناتِ:

1. **البياناتُ (Data)**: تشكلُ البياناتُ بجميعِ أشكالِها (نصٍّ، صورةٍ، صوتٍ، فيديو) أساسَ نظامِ الذكاءِ الاصطناعيِّ، وتُستخدمُ البياناتُ كمدخلاتٍ للنظامِ لتدريبِ الخوارزمياتِ على تعرُّفِ الأنماطِ وتوليدِ المخرجاتِ، وتشملُ مكوناتٍ متخصصةً لتحليلِ البياناتِ، مثلَ معالجةِ اللغةِ الطبيعيةِ (NLP) والرؤيةِ الحاسوبيةِ.
2. **الخوارزمياتُ (Algorithms)**: هيَ سلسلةٌ منَ الخطواتِ المنطقيةِ التي تستخدمُ لتحليلِ البياناتِ في الذكاءِ الاصطناعيِّ، تقومُ الخوارزمياتُ باكتشافِ الأنماطِ منَ البياناتِ، وتستخدمُ هذهِ الأنماطُ لتوليدِ المخرجاتِ، وربطِ المدخلاتِ بالنتائجِ.
3. **النماذجُ (Models)**: تمثلُ النماذجُ المعرفةَ المستخرجةَ منَ البياناتِ بعدَ تطبيقِ الخوارزمياتِ، وهذهِ النماذجُ قادرةٌ على التنبؤِ أوِ اتخاذِ القراراتِ بناءً على معلوماتٍ جديدةٍ.

إضاءةٌ

تعلمتَ في مبحثِ الرياضياتِ كيفيةَ تفسيرِ التمثيلاتِ البيانيةِ للعلاقاتِ، فالتمثيلُ البيانيُّ للعلاقاتِ في الرياضياتِ يوضحُ كيفيةَ ارتباطِ المفاهيمِ بعضِها ببعضٍ بشكلٍ مشابهٍ لما يحدثُ في نظامِ الذكاءِ الاصطناعيِّ.

التمثيلُ البيانيُّ: يمثلُ المدخلاتِ التي يُغذي بها النظامَ.

الخطواتُ أو العملياتُ الرياضيةُ: تشبهُ الخوارزمياتِ المستخدمةَ لتحليلِ البياناتِ وتحديدِ الأنماطِ.

التفسيراتُ: تشبهُ المخرجاتِ التي يُنتجها النظامُ بعدَ تطبيقِ الخوارزمياتِ.

أبحثُ

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عن الاستخدامِ الأوليِّ للذكاءِ الاصطناعيِّ، وأكتبُ تقريرًا باستخدامِ تطبيقِ (Google Docs)، وأشاركُهُ معَ زملائي على اللوحِ التفاعليِّ للصفِّ (Padlet)؛ لمناقشةِ ما توصلتُ إليهِ.

إثراء

يوجدُ عديدٌ منَ الخوارزمياتِ المستخدمةِ في الذكاءِ الاصطناعيِّ، منها:

الانحدارُ الخطيُّ (Linear Regression) ،
والانحدارُ اللوجستيُّ (Logistic Regression)،
وشجرةُ القرارِ (Decision Tree).

منْ أشهرِ النماذجِ المستخدمةِ في الذكاءِ الاصطناعيِّ:

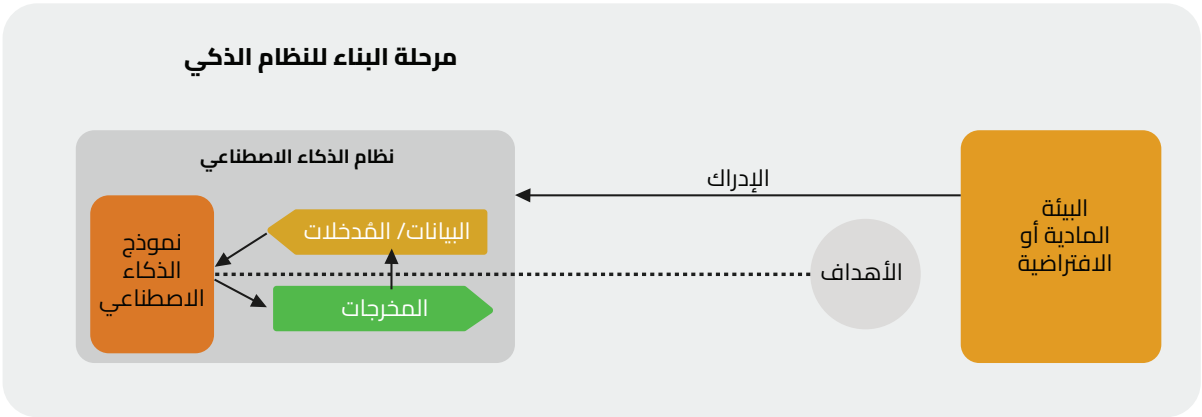
الشبكةُ العصبيةُ الاصطناعيّةُ (Artificial Neural Network – ANN) ،
والشبكةُ العصبيةُ الالتفافيةُ (Convolutional Neural Network – CNN)،
والشبكةُ العصبيةُ المتكرّرةُ (Recurrent Neural Network – RNN).

مراحلُ إعدادِ نظامِ الذكاءِ الاصطناعيِّ

يَمرُّ نظامُ الذكاءِ الاصطناعيِّ بمرحلتيْنِ أساسيتيْنِ، هما: مرحلةُ البناءِ، ومرحلةُ الاستخدامِ.

أوّلًا: مرحلةُ البناءِ:

تتضمنُ هذهِ المرحلةُ عملياتِ جمعِ البياناتِ ومعالجتِها، واختيارَ الخوارزمياتِ، وتدريبَ النموذجِ، واختبارَ النموذجِ. انظرِ الشّكلَ (1-1).



الشكل (1-1): مرحلة البناء في الذكاء الاصطناعي

في ما يأتي توضيحٌ لهذهِ العملياتِ:

1. **جمعُ البياناتِ (Data Collection):**

تبدأُ العملياتُ في مرحلةِ البناءِ بجمعِ البياناتِ اللازمةِ للنظامِ؛ إذْ يُمكنُ أنْ تكونَ هذهِ البياناتُ نصوصًا، أوْ صورًا، أوْ أصواتًا، أوْ أيَّ شكلٍ آخرَ منَ البياناتِ الرَّقْميةِ التي تعكسُ البيئةَ أوِ المشكلةَ التي يهدفُ النظامُ إلى معالجتِها.

2. **معالجةُ البياناتِ (Data Preprocessing):**

في هذهِ المرحلةِ، تُنظَّفُ البياناتُ وتُنقَّحُ منَ الأخطاءِ أوِ القيمِ المفقودةِ أوِ القيمِ المكرّرةِ، وتُطبَّعُ أو تُحَوَّلُ إلى صيغةٍ ملائمةٍ لتدريبِ النموذجِ، ويمكنُ أنْ تشتملَ هذهِ المرحلةُ أيضًا عمليةَ اختيارِ الميزاتِ الأكثرِ تأثيرًا في أداءِ النموذجِ.

3. **اختيارُ الخوارزمياتِ (Algorithm Selection):**

بناءً على نوعِ المشكلةِ والبياناتِ المتاحةِ، تُختارُ الخوارزميةُ المناسبةُ، وتَختلفُ الخوارزمياتُ وَفْقًا للمهامِّ، مثلَ التصنيفِ، أوِ التنبؤِ، أوِ التّعرفِ إلى الأنماطِ، أوْ تمييزِ الأصواتِ وغيرِها.

4. **تدريبُ النموذجِ (Model Training):**

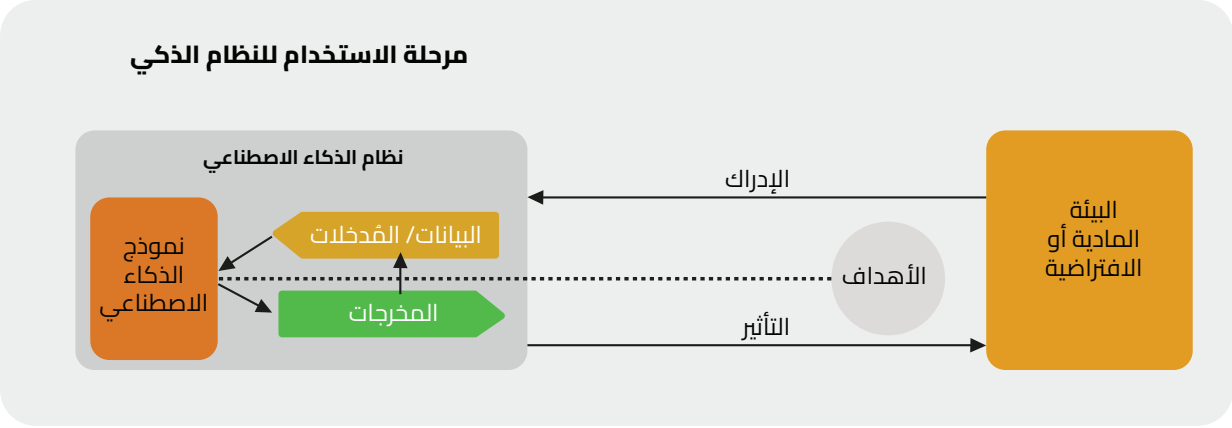
يتمُّ تدريبُ النموذجِ باستخدامِ البياناتِ المعالجةِ لتعلّمِ الأنماطِ والعلاقاتِ بينَ البياناتِ، وخلالَ هذهِ المرحلةِ يتعلّمُ النموذجُ كيفيةَ اتخاذِ القراراتِ أوْ تقديمِ التوقعاتِ بناءً على البياناتِ المقدمةِ لهُ، وتعدُّ عمليةُ تدريبِ النظامِ الذكيِّ المِفتاحَ الأساسيَّ لعمليةِ التعلّمِ؛ حيثُ تُعطى كميةٌ كبيرةٌ منَ البياناتِ، ومجموعةٌ من التعليماتِ للنظامِ، وقد تكونُ التعليماتُ عملياتِ تصنيفٍ، أوْ بحثًا عنْ صورٍ تُحقّقُ شرطًا معينًا، فيعملُ النظامُ على البحثِ عنِ الأنماطِ في البياناتِ المقدمةِ لهُ.

5. **اختبارُ النموذجِ (Model Testing):**

بعدَ التدريبِ، يُختبرُ النموذجُ باستخدامِ مجموعةِ بياناتٍ جديدةٍ لمْ يستخدمْها في مرحلةِ التدريبِ، والهدفُ منها هوَ تقييمُ دقةِ النموذجِ وقدرتِهِ على التعميمِ عندَ التعاملِ معَ بياناتٍ جديدةٍ، وإذا كانَ الأداءُ أقلَّ منَ المتوقعِ، يتمُ تحسينُ أيٍّ منَ الخطواتِ السابقةِ.

ثانيًا: مرحلةُ الاستخدامِ

تتضمنُ هذهِ المرحلةُ عملياتِ الاستدلالِ باستخدامِ النموذجِ على بياناتٍ جديدةٍ، ونشرِ النموذجِ المدرّبِ، وتَلقّي التغذيةِ الراجعةِ لتحسينِ الأداءِ بشكلٍ مستمرٍ، وفي هذهِ المرحلةِ يكونُ نظامُ الذكاءِ الاصطناعيِّ متاحًا للمستخدمين، حينئذٍ لا بدَّ منْ وجودِ عناصرِ تحكّمٍ لوصولِ المستخدمينَ للنظامِ، منْ ثمَّ تتبعُ جودةِ تجربةِ المستخدمِ عبرَ مؤشراتِ أداءٍ. (تُسمى هذهِ المرحلةُ التقييمَ منْ أجلِ التحسينِ). انظرِ الشكلَ (1-2).



الشكل (1-2): مرحلة الاستخدام في أنظمة الذكاء الاصطناعي

وفي ما يأتي توضيحٌ لهذهِ العملياتِ:

1. **التنبؤُ أوِ الاستدلالُ (Inference):**

بعدَ التدريبِ والاختبارِ، يصبحُ النموذجُ جاهزًا للاستخدامِ في الحياةِ العمليةِ؛ حيثُ يُستخدمُ النموذجُ لاتخاذِ قراراتٍ أوْ تقديمِ توقعاتٍ، استنادًا إلى بياناتٍ جديدةٍ تُدخَلُ إليهِ.

إضاءةٌ

تُصنَّفُ الاستدلالاتُ في المنطقِ إلى استقرائيةٍ أوِ استنتاجيةٍ أوِ احتماليةٍ. في الاستدلالِ الاستقرائيِّ، يتمُ جمعُ البياناتِ وتطويرُ نماذجَ مؤقتةٍ لوصفِ السلوكِ المستقبليِ والتنبؤِ بهِ؛ أيْ أنَّه يعتمدُ على الانتقالِ منَ الخاصِّ إلى العامِّ (منْ ملاحظاتٍ محددةٍ إلى تعميماتٍ أوسعَ)، في حينٍ، يُنتقَلُ منَ العامِّ إلى الخاصِّ (منَ التعميمِ إلى التخصيصِ) في الاستدلالِ الاستنتاجيِّ. أما الاستدلالُ الاحتماليُّ، فيعتمدُ على نماذجَ احتماليةٍ للتعاملِ معَ المعلوماتِ غيرِ المؤكدةِ أوِ الناقصةِ، ويُستخدمُ هذا النوعُ من الاستدلالِ في التعاملِ معَ البيئاتِ المعقدةِ، أوْ عندما تكونُ المعلوماتُ غيرَ مكتملةٍ.

2. **النشرُ (Deployment):**

بعدَ التأكدِ منْ أنَّ النظامَ يعملُ بشكلٍ جيّدٍ، يُنشَرُ ليصبحَ متاحًا للاستخدامِ الفعليِّ، ويمكنُ أنْ يكونَ هذا النظامُ جزءًا منْ تطبيقٍ، أوْ منصةَ خدماتٍ، أوْ نظامًا مستقلًا يتفاعلُ معَ المستخدمينَ.

3. **التحسينُ والتغذيةُ الراجعة (Optimization and Feedback):**

استنادًا إلى أداءِ النظامِ، تُجمعُ التغذيةُ الراجعةُ لتحديثِ النموذجِ وتحسينِهِ، وقدْ تشملُ هذهِ المرحلةُ إعادةَ تدريبِ النموذجِ على بياناتٍ جديدةٍ، أوْ تحسينِ الخوارزمياتِ المستخدمةِ، وهيَ عمليةٌ مستمرةٌ.

نشاط جماعي

أتأملُ وأفسرُ

أتأملُ الشّكليْنِ (1-1) و(1-2)، وأفسرُ دلالةَ مصطلحي الإدراكِ والتأثيرِ المُبيّنةِ في الشكليْنِ، ثمَّ أستخدمُ المصادرَ المتاحةَ للبحثِ عنْ دلالتِهما، وأشاركُ ما توصلتُ إليهِ معَ زملائي في المجموعاتِ الأخرى.

خصائصُ أنظمةِ الذكاءِ الاصطناعيِّ

تشمُل خصائصُ أنظمةِ الذكاءِ الاصطناعيِّ مجموعةً منَ القدراتِ والمميزاتِ التي تجعلُها مميزةً عنِ الأنظمةِ التقليديةِ. في ما يأتي أهمُّ هذهِ الخصائصِ:

1. **التعلّمُ (Learning):** يشيرُ إلى قدرةِ النظامِ الذكي على تحسينِ أدائِهِ عبرَ اكتسابِ المعرفةِ منَ البياناتِ أوِ التجاربِ السابقةِ، ويمكنُ أنْ يكونَ التعلّمُ تحتَ إشرافٍ، أوْ غيرَ خاضعٍ للإشرافِ، أوْ معززًا.

2. **التكيُّفُ (Adaptation):** قدرة الانظمة الذكية علي التكيّفُ معَ الظروفِ الجديدةِ، والبياناتِ المتغيرةِ منْ دونِ الحاجةِ لإعادةِ البرمجةِ.

3. **الاستدلالُ (Reasoning):** قدرةُ النظامِ الذكي على استنتاجِ نتائجَ جديدةٍ باستخدامِ القواعدِ المنطقيةِ أوِ الاحتمالاتِ بناءً على المعلوماتِ المتاحةِ.

4. **المرونةُ (Flexibility):** قدرة النظامِ الذكي على التعاملِ معَ مهامَّ مختلفةٍ في مجالاتٍ متعددةٍ، مثلَ الرعايةِ الصحيةِ، والماليةِ، والنقلِ، والترفيهِ.

5. **التخطيطُ وحلُّ المشـــكلاتِ (Planning and Problem Solving)**: قدرةُ النظامِ الذكي على تحديدِ الأهدافِ، ووضعِ الاستراتيجياتِ والخطواتِ لتحقيقِها، وتجاوزِ العقباتِ للوصولِ إلى النتائجِ المطلوبةِ.

6. **التمثيلُ المعرفيُّ(Knowledge Representation)**: هوَ الطريقةُ التي يتمُ فيها تخزينُ المعلوماتِ والمعرفةِ في النظامِ الذكي؛ بحيثُ يمكنُ استخدامُها للاستدلالِ واتخاذِ القراراتِ.

7. **أتمتةُ المهامِّ (Automate Tasks)**: تتعاملُ أنظمةُ الذكاءِ الاصطناعيِّ معَ المهامِّ على اختلافِ تعقيداتِها، ثمَ إنَّ اســـتخدامَها يُحوّلُ الأنشطةَ اليدويةَ إلى أنشطةٍ حاسوبيةٍ تأخذُ وقتًا وجهدًا أقلَّ بكثيرٍ.

8. **استيعابُ البياناتِ (Data Ingestion)**: تعملُ أنظمةُ الذكاءِ الاصطناعيِّ على جمعِ العددِ الكبيرِ منَ البياناتِ، وتحليلِ هذهِ البياناتِ وتفسيرِها بما يتناسبُ معَ الخبراتِ السابقةِ، منْ ثمَّ توليدُ المعرفةِ. منَ الأمثلةِ عليها: قدرةُ بعضِ الأنظمةِ الذكية على جمعِ بياناتِ مستخدمي الإنترنتِ وتحليلِها لمعرفةِ توجيهاتِهمُ الاستهلاكيةِ.

9. **التفاعلُ معَ البيئةِ (Interaction with Environment)**: قدرةُ الأنظمةِ الذكية على التفاعلِ مع بيئاتٍ ديناميكيةٍ، سواءٌ أكانتْ ماديةً أو رقميةً، والتواصلِ معَ المستخدمينَ بطرقٍ مفيدةٍ وهادفةٍ.

10. **التفاعلُ الطبيعيُّ (Natural Interaction)**: دعمُ التفاعلِ معَ البشرِ باستخدامِ اللغاتِ الطبيعيةِ (مثلَ معالجةِ اللغةِ الطبيعيةِ (NLP) ، والتعاملِ معَ الوســـائطِ المتعددةِ كالصورِ والنصوصِ والصوتِ

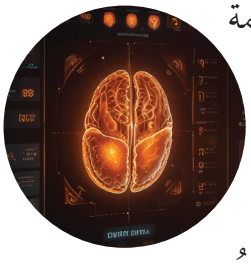
نشاط عملي

أستخدمُ تطبيقَ الذكاءِ الاصطناعيِّ (ChatGPT) للمقارنةِ بينَ أنظمةِ الذكاءِ الاصطناعيِّ والأنظمةِ التقليديةِ. بعدَ الانتهاءِ من المقارنةِ، أناقشُ النتائجَ التي توصلتُ إليها معَ زملائي، وأقارن هلْ توصلَ الجميعُ إلى النتائجِ نفسِها، ثمَّ أفسرُ سببَ التشابُهِ أوِ الاختلافِ في النتائجِ بناءً على التحليلاتِ المختلفةِ التي قمْنا بِها، ووجهاتِ النظرِ التي تمَّ تناولُها.

أمثلةٌ على أنظمةِ الذكاءِ الاصطناعيِّ:

1. **أنظمةُ ذكاءٍ اصطناعيٍّ خاصةٍ بالتعليمِ**: منَ الأمثلةِ عليها؛ المعلمونَ الافتراضيونَ مثلَ Squirrel AI، ومنصاتٍ مثلَ Khan Academy التي تستطيعُ تخصيصَ تجاربِ التعلّمِ للطلبةِ.

2. **مساعداتُ الصوتِ الذكيةِ (Smart Voice Assistants)**: تُستخدمُ تِقْنيّاتُ معالجةِ اللغةِ الطبيعيةِ لفهمِ أوامرِ المستخدمِ الصوتيةِ والردِّ عليها، ويمكنُها إجراءُ عملياتِ بحثٍ، وضبطُ المواعيدِ، والتحكمُ في الأجهزةِ المنزليةِ الذكيةِ، وتقديمُ التوصياتِ بناءً على تفضيلاتِ المستخدمِ. منْ أمثلتِها: Google Assistant، Alexa (Amazon)، Siri (Apple).



3. **أنظمةُ التشخيصِ الطبيِّ (Medical Diagnosis Systems)**: تَستخدمُ أنظمةُ التشخيصِ الطبيِّ الذكاءَ الاصطناعيَّ لتحليلِ بياناتِ المرضى، والتعرّفِ إلى الأنماطِ في الصورِ الطبيةِ، وتقديمِ توصياتٍ حوَلَ التشخيصِ والعلاجِ، ويمكنُها تحسينُ دقةِ التشخيصِ، وتقليلُ الوقتِ اللازمِ لاتخاذِ القراراتِ الطبيةِ. منْ أمثلتِها: IBM Watson for Oncology الذي يساعدُ الأطباءَ في اختيارِ العلاجاتِ المناسبةِ للسرطانِ بناءً على تحليلِ بياناتِ المرضى والمراجعِ الطبيةِ.

4. **الروبوتاتُ الصناعيةُ (Industrial Robots)**: تُستخدمُ هذهِ الروبوتاتُ في البيئاتِ التصنيعيةِ لأداءِ المهامِّ المتكررةِ والصعبةِ بكفاءةٍ عاليةٍ، ويمكنُ برمجتُها أوْ تعليمُها باستخدامِ تِقْنيّاتِ التعلّمِ المعزّزِ لتحسينِ أدائِها بمرورِ الوقتِ. منْ أمثلتِها: Fanuc Robotics الذي يقدمُ حلولًا لمختلفِ التطبيقاتِ الصناعيةِ.

أبحث

أبحثُ في المصادرِ الإلكترونيـــةِ الموثوقةِ عنْ أمثلةٍ أُخرى لأنظمـــةِ الذكاءِ الاصطناعيِّ، وأُشاركُها زملائي باستخدامِ اللوحِ التفاعليِّ للصفِّ Padlet

نشاط جماعي

أحلِّلُ وأستنتجُ

أتعاونُ مـــعَ زملائي في المجموعةِ لتحليلِ الأمثلةِ المذكورةِ على أنظمةِ الذكاءِ الاصطناعيِّ، وأستنتجُ ما إذا كانتْ هذهِ الأنظمةُ تمتلكُ خصائصَ ومميزاتٍ مشتركةً. بعدَ ذلكَ، نناقشُ هذهِ الخصائصَ والمميزاتِ، ونحـــدّدُ بعضًا منها بالتوافقِ. في النهايةِ، نعرضُ ما توصلْنا إليهِ أمامَ المجموعاتِ الأخرى، ونتبادلُ الأفكارَ والنقاشَ.

مراحلُ تطورِ الذكاءِ الاصطناعيِّ

تطـــوَّرَ الذكاءُ الاصطناعيُّ (AI) عبرَ مراحلَ عدةٍ منذُ عقدِ الســـبعينياتِ حتى عصرِنا هذا، ويمكنُ تصنيفُ هذهِ المراحلِ إلى فتراتٍ رئيســـةٍ بناءً على التقدمِ التكنولوجيِّ والتِّقْنيِّ، والنهجِ المستخدمِ لتطويرِ النماذجِ.

عرضٌ لهذهِ المراحلِ وأبرزِ ما يُميزُها:

نشأةُ الذكاءِ الاصطناعيِّ (الخمسينيّاتُ والســـتينيّاتُ): مَثلتْ هذهِ المرحلةُ بدايةَ التفكيرِ في الذكاءِ الاصطناعيِّ بوصفِه نظامًا قادرًا على محاكاةِ التفكيرِ البشريِّ؛ إذْ بدأتِ الأفكارُ تتبلورُ حولَ إمكانيةِ صنعِ آلاتٍ قادرةٍ على "التفكيرِ" أو "التعلّمِ".

الذكاءُ الاصطناعـــيُّ الرمزيُ (الســـبعينيّاتُ والثمانينيّـــاتُ): كانَ الذكاءُ الاصطناعيُّ في هذهِ المرحلةِ يعتمدُ بشـــكلٍ أساسيٍّ على القواعدِ والرموزِ؛ حيثُ اعتمدتِ النُّظمُ على البرمجةِ الصريحةِ للمعلوماتِ والمعرفةِ.

الذكاءُ الاصطناعيُّ القائمُ على التعلّمِ (التسعينيّاتُ): ظهرَ مفهومُ التعلّمِ الآليِّ؛ حيثُ بدأَ استخدامُ الخوارزمياتِ لتدريبِ النماذجِ للتعرّفِ إلى الأنماطِ منَ البياناتِ.

الذكاءُ الاصطناعيُّ العميقُ (الألفيةُ الجديدةُ): ظهرَ التعلّمُ العميقُ الذي يعتمدُ على الشبكاتِ العصبيةِ المتعددةِ الطبقاتِ (Deep Neural Networks) ومنْ أبرزِ ما ميّزَ هذهِ المرحلةَ التطورُ الكبيرُ في القدراتِ الحاسوبيةِ، وتوافرُ كمياتٍ ضخمةٍ من البياناتِ.

الذكاءُ الاصطناعيُّ القابلُ للتفسيرِ (2020s): يتميزُ بالتركيزِ على تطويرِ نماذجِ ذكاءٍ اصطناعيٍّ، يمكنُ تفسيرُها وفهمُها منْ قبلِ البشرِ؛ لضمانِ الشفافيةِ والعدالةِ في القراراتِ.

الذكاءُ الاصطناعيُّ المعزّزُ (المستقبلُ القريبُ): دُمجَ الذكاءِ الاصطناعيِّ بمهاراتٍ وقدراتٍ بشريةٍ متقدمةٍ، لتحسينِ تفاعلِ الإنسانِ معَ الآلةِ بطرقٍ جديدةٍ أكثرَ تفاعليةٍ.

نشاط جماعي

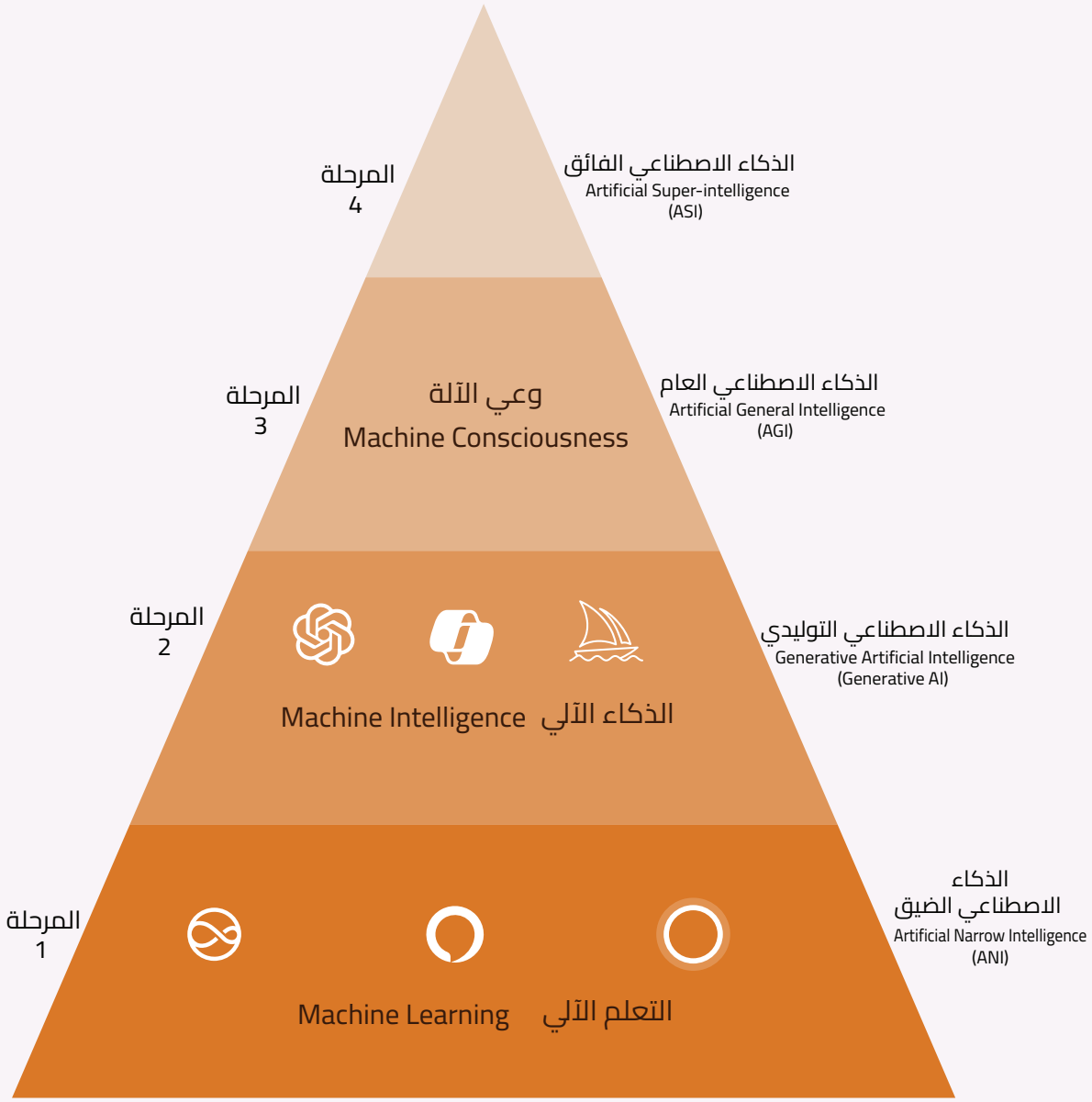
أبحثُ وأقارنُ

تعرَّضَ علمُ الذكاءِ الاصطناعيِّ لانتكاستيْنِ انخفضتْ فيهما البحوثُ الخاصّةُ بهِ، وسُميتِ الانتكاسةُ الأولى بالشتاءِ الأوّلِ للذكاءِ الاصطناعيِّ، في حينِ سُميتِ الانتكاسةُ الثانيةُ باسمِ الشتاءِ الثاني للذكاءِ الاصطناعيِّ. أبحثُ وزملائي عنْ هاتيْنِ الفترتيْنِ، وعنِ الأسبابِ التي أدّتْ إلى ذلكَ، مثلَ التحدياتِ التِّقْنيّةِ والتوقعاتِ غيرِ الواقعيةِ. بعدَ ذلكَ، نعملُ على تصميمِ إنفوجرافيك باستخدامِ (Canva) لعرضِ النتائجِ بطريقةٍ بصريةٍ واضحةٍ، ثمَّ نعرضُ هذا العملَ على اللوحِ التفاعليِّ للصفِّ (Padlet)، ونقارنُ إجابتَنا معَ إجاباتِ المجموعاتِ الأخرى؛ لنرى إنْ كانتِ النتائجُ متشابهةً، وهلْ جميعُ المجموعاتِ قدّمتِ النتائجَ نفسَها، ثمَّ أفسرُ ذلكَ.

إثراء

مستوياتُ الذكاءِ الاصطناعيِّ (أنواعُ الذكاءِ الاصطناعيِّ)

الشكل (1–3)) يوضّحُ تصنيفَ الذكاءِ الاصطناعيِّ إلى مستوياتٍ مختلفةٍ، تعتمدُ على قدراتِهِ والأدوارِ التي يمكنُ أنْ يؤديها. في ما يأتي توضيحٌ لهذِهِ المستوياتِ:



الشكل (1–3) : مستويات الذكاء الاصطناعي

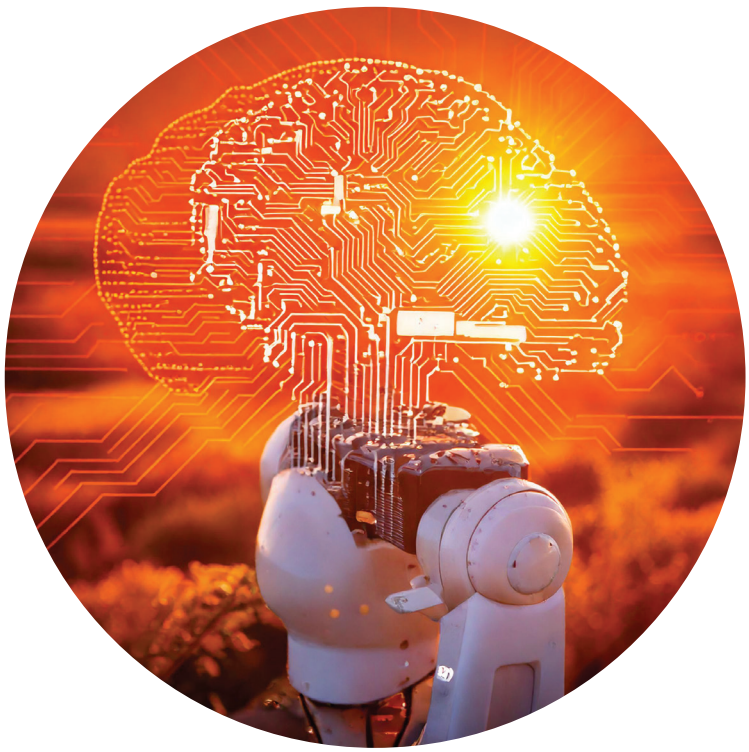
نشاط جماعي

أستنتجُ أهميةَ الذكاءِ الاصطناعيِّ منَ المعلوماتِ الواردةِ في الدرسِ، ثمَّ أبحثُ في المصادرِ المتاحةِ، مثلَ المقالاتِ العلميةِ والدراساتِ الموثوقةِ؛ للعثورِ على نقاطٍ إضافيةٍ تبيّنُ تأثيرَ الذكاءِ الاصطناعيِّ وفوائدَهُ وأهميتَهُ، وأُلخّصُ النتائجَ في مستندِ (Google Docs)، وأُشاركُهُ على اللوحِ الرَّقْميِّ التفاعليِّ للصفِّ (Padlet)؛ حيثُ يمكنُ لي ولزملائي الاطّلاعُ عليهِ، والتفاعلُ معَ المحتوى المقدَّمِ.

المُواطَنةُ الرَّقْميةُ

أراعي عندَ استخدامِ برامجِ الذكاءِ الاصطناعيِّ ومحركاتِ البحثِ ما يأتي:

- **توثيقَ المعلوماتِ:** أُوثّقُ المعلوماتِ التي حصلتُ عليها منْ مواقعِ البحثِ.
- **المشاركةَ:** أشاركُ زملائي المعلوماتِ الصحيحةَ والحديثةَ التي اطّلعتُ عليها.
- **الاستخدامَ المسؤولَ:** أستخدمُ التكنولوجيا في كلِّ ما هوَ مفيدٌ، وأتجنبُ استخدامَها في الأمورِ المؤذيةِ والسيئةِ.
- **التفاعلاتَ الإيجابيةَ:** أحترمُ وجهةَ نظرِ زميلي المؤيدةِ أوِ المعارضةِ، وأُناقشُ عنْ طريقِ تقديمِ الأدلةِ التي تدعمُ وجهةَ نظري.
- **التعليمَ المستمرَ:** أُشجعُ على تصميمِ برامجِ ذكاءٍ اصطناعيٍّ تعملُ على تحسينِ حياةِ الإنسانِ.



مشروع

المشروعُ: إنتاجُ سلسلةٍ منْ مقاطعِ الفيديو التعليميةِ (الرسومِ المتحركةِ) على شكلِ حلْقاتٍ؛ حيثُ تتناولُ كلُّ حلْقةٍ موضوعًا محددًا، باستخدامِ تطبيقاتِ الذكاءِ الاصطناعيِّ/ المهمةُ 1.

أبدأُ معَ أفرادِ مجموعتي التحضيرَ والتخطيطَ لإعدادِ سلسلةِ حلْقاتٍ تعليميةٍ (الرسومِ المتحركةِ)، وذلكَ بالتحضيرِ والتخطيطِ لسلسلةِ حلْقاتٍ تعليميةٍ على النحوِ الآتي:

- **التحضيرُ للأفكارِ واختيارُ الموضوعاتِ:** نُنسقُ معَ المجموعاتِ الأخرى لتحديدِ الموضوعاتِ بشكلٍ يضمنُ عدمَ التكرارِ.
- **تخطيطُ السيناريو للفيديوهاتِ:**
  - إعدادُ لوحةٍ قصصيةٍ تتضمنُ تحديدَ الشخصياتِ، والحوارَ المكتوبَ والمسموعَ، والخلفياتِ.
  - استخدامُ الذكاءِ الاصطناعيِّ لاختيارِ الشخصياتِ عبرَ موقعِ (lexica.art) وحفظِها بعدَ إزالةِ الخلفياتِ باستخدامِ (Photopea.com) .
- توزيعُ المهامِّ، وتحديدُ الزمنِ المطلوبِ لإنجازِ كلِّ جزءٍ منَ المشروعِ.
- إنتاجُ الحلْقةِ الأولى التي تُركّزُ على "مفهومِ الذكاءِ الاصطناعيِّ ومكوناتِهِ".
  - **التعليماتُ العامّةُ لإنجازِ الحلْقاتِ:**
    - استخدامُ (www.d-id.com) لجعلِ الشخصياتِ تتحدثُ.
    - استخدامُ (Kapwing.com) لإزالةِ الخلفيةِ الخضراءِ منَ الفيديوهاتِ.
    - استخدامُ برنامجِ (moviemaker) لإنتاجِ الفيديو النهائيِّ.

أدواتُ ومواقعُ الذكاءِ الاصطناعيِّ، يمكنُ الاستفادةُ منها في ما يأتي:

- استخدامُ مواقعَ مثلَ (lumen5.com)، (ai.invideo.io)، (Kapwing.com)، لإنشاءِ مقاطعِ الفيديو.
- استخدامُ (www.d-id.com) لتحريكِ الشخصياتِ بالذكاءِ الاصطناعيِّ.
- استخدامُ (www.convert. leiapix.com)لإنشاءِ خلفياتٍ متحركةٍ وواقعيةٍ.
- استخدامُ مواقعَ مثلَ (Photopea.com)، (gimp.org)، (Ping create.ai)، (Leonardo.ai)، لتحريرِ الصورِ.
- استخدامُ مواقعَ مثلَ (Voicemaker.in)، (Ttsreader.com)، (Naturalreaders.com)، (Balabolka.org) لتحويلِ النّصِّ إلى صوتٍ.

أقيّمُ تعلُّمي

المعرفةُ: أُوظفُ في هذا الدرسِ ما تعلمتُهُ منْ معارفَ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأوّلُ: أُعرِّفُ الذكاءَ الاصطناعيَّ مبينًا أهميتَهُ.

.....

السؤالُ الثاني: أذكرُ خصائصَ الذكاءِ الاصطناعيِّ معَ توضيحِ كلٍّ منها.

.....

السؤالُ الثالثُ: أرسمُ مخططًا يبيّنُ مرحلةَ البناءِ في أنظمةِ الذكاءِ الاصطناعيِّ.

.....

السؤالُ الرّابعُ: أكتبُ المصطلحَ الصّحيحَ بجانبِ كلِّ عبارةٍ في ما يأتي:

1. ( ): ظهرَ فيهِ مفهومُ التعلّمِ الآليِّ؛ حيثُ بدأَ استخدامُ الخوارزمياتِ لتدريبِ النماذجِ على تعرُّفِ الأنماطِ منَ البياناتِ.
2. ( ): منَ الأمثلةِ عليها: أنظمةُ التعرّفِ إلى الوجهِ، والمَركباتُ ذاتيةُ القيادةِ، والتصويرُ الطبيُّ.
3. ( ): تتضمنُ هذهِ المرحلةُ عملياتِ نشرِ النموذجِ المدرّبِ، والاستدلالَ باستخدامِ النموذجِ على بياناتٍ جديدةٍ، وتلقي التغذيةِ الراجعةِ لتحسينِ الأداءِ بشكلٍ مستمرٍ.

المهاراتُ: أُوظفُ مهاراتِ التفكيرِ الناقدِ، والتواصلَ الرَّقْميَّ، والبحثَ الرَّقْميَّ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأوّلُ: أُصنّفُ المهامَّ الآتيةَ إلى مهامَّ تحتاجُ إلى الذكاءِ الاصطناعيِّ بوضعِ إشارة (✔) بجانبها، ومهامَّ لا تحتاجُ إلى ذكاءٍ اصطناعيٍّ بوضعِ إشارة (✖).

- ☐ استخدامُ جداولِ إكسل لحسابِ معدلِ الطالبِ، ومعدلِ علاماتِ الطلبةِ في شعبةٍ معينةٍ، ومقارنتِها بالشّعَبِ الأخرى.
- ☐ استخدامُ Google Map للحصولِ على أسرعِ طريقٍ.
- ☐ تخزينُ كمياتٍ كبيرةٍ منَ الأفلامِ وبثها للمشاهدينَ في الوقتِ نفسِهِ.
- ☐ استخدامُ برامجِ تحريرِ الصورِ والفيديو لتعديلِ الألوانِ.
- ☐ استخدامُ الفلاترِ في الصورِ.
- ☐ التنبؤُ بحالةِ الطقسِ مدةُ شهرٍ.

السـؤالُ الثاني: أُميزُ بينَ أنظمةِ الذكاءِ الاصطناعيِّ والأنظمةِ الحاسوبيةِ التقليديةِ بناءً على دراستي لعناصرِ أنظمةِ الذكاءِ الاصطناعيِّ ومكوناتِها وخصائِصِهـا، وأُرتبُ أفكاري في نقاطٍ، ثمَّ أُصممُ منشورًا خاصًّا بذلكَ.

السـؤالُ الثالثُ: أبحثُ عنْ تطبيقاتِ ذكاءٍ اصطناعيٍّ استُخدمتْ في مجالِ التعليمِ، وأكتبُ تقريرًا عنها.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

القيمُ والاتجاهاتُ:

أُعدُّ برنامجًا إذاعيًّا لنشرِ الوعيِ بأهميةِ اسـتخدامِ أنظمةِ الذكاءِ الاصطناعيِّ ومخاطرِهِ، وأُدقّقُهُ معَ معلمي، ثمَّ أُقدمُهُ في برنامجِ الإذاعةِ الصباحيِّ.

الدرسُ الثاني

تطبيقاتُ الذكاءِ الاصطناعيِّ
(Applications of Artificial Intelligence)

الفكرةُ الرئيسةُ

التعرُّفُ إلى تطبيقاتِ الذكاءِ الاصطناعيِّ في مجالاتِ الحياةِ المختلفةِ، وتأثيرِ تبنّي هذهِ التِقْنيّاتِ في تطويرِ كفاءةِ العملِ في كلِّ مجالٍ. بالإضافةِ إلى تعرُّفِ ماهيةِ تأثُّرِ المجتمعِ والأفرادِ بهذهِ التطبيقاتِ.

المفاهيمُ والمصطلحاتُ

الرعايةُ الصحيّةُ (Healthcare)، التجارةُ (Retail)، الصناعةُ (Manufacturing)، النقلُ (Transportation)، ذكاءُ الأعمالِ (Business Intelligence)، التأثيراتُ الاجتماعيةُ (Social Impact).

نتاجاتُ التعلّمِ (Learning Outcomes)

- أتعرف تطبيقات الذكاء الاصطناعي.
- أُوضّحُ مجالاتِ تطبيقِ الذكاءِ الاصطناعيِّ في النُّظمِ المعرفيةِ الأخرى.
- أُوضحُ تطبيقاتِ الذكاءِ الاصطناعيِّ.
- أُحدّدُ الآثارَ الاجتماعيةَ للذكاءِ الاصطناعيِّ.

منتجاتُ التعلّمِ
(Learning Products)

إعدادُ لوحاتٍ قصصيةٍ (Storyboards) تفصيليةٍ أساسيةٍ للحلْقةِ الثانيةِ منْ سلسلةِ الفيديوهاتِ، وإنتاجها باستخدامِ مواقعَ وتطبيقاتِ الذكاءِ الاصطناعيِّ.

بعدَ أنْ تعرَّفنا إلى الذكاءِ الاصطناعيِّ ومفهومِهِ وأهميتِهِ وخصائصِهِ ومراحلِ تطورِهِ، لا بدَّ منْ معرفةِ تطبيقاتِهِ الحياتيةِ. فهلْ تقتصرُ هذهِ التطبيقاتُ على مجالاتٍ محدّدةٍ؟ وهلْ هيَ موجهةٌ إلى فئةٍ معينةٍ؟

نشاط تمهيدي

هلْ سبقَ أنْ استخدمتُ في حياتي اليوميةِ وسائلَ تَستعملُ الذكاءَ الاصطناعيَّ؟ كيفَ أميزُها عنِ الأنظمةِ غيرِ الذكيةِ؟ ما الفوائدُ التي قدمَتْها لي تلكَ الوسائلُ؟ أشاركُ تجربتي معَ زملائي في الصفِّ.

مجالاتُ تطبيقِ الذكاءِ الاصطناعيِّ

يُستخدمُ الذكاءُ الاصطناعيُّ في مجموعةٍ واسعةٍ منَ المجالاتِ؛ لتحسينِ الكفاءةِ، وتقديمِ حلولٍ مبتكرةٍ، وتسهيلِ عملياتِ اتخاذِ القرارِ، وقدْ اكتسبَ الذكاءُ الاصطناعيُّ هذهِ الأهميةَ؛ بسببِ وجودِ كمياتٍ كبيرةٍ منَ المعلوماتِ، والتطورِ الكبيرِ في سرعةِ الحواسيبِ والمسرِّعاتِ التي إنْ دُمِجتْ معَ خوارزمياتِ الذكاءِ الاصطناعيِّ الفعالةِ؛ حيثُ ستعطي هذهِ الخوارزمياتِ القدرةَ على قراءةِ البياناتِ والنصوصِ والصورِ وتحليلِها، واتخاذِ القرارِ المناسبِ بسرعةٍ كبيرةٍ ودقةٍ عاليةٍ.

سنتعرّفُ في ما يأتي إلى أبرزِ هذهِ المجالاتِ:

التعليمُ

يتمتعُ الذكاءُ الاصطناعيُّ بالقدرةِ العاليةِ على معالجةِ كمياتٍ كبيرةٍ منَ البياناتِ وتحليلِها؛ ممّا يقدمُ العديدَ منَ الفرصِ الواعدةِ لقطاعِ التعليمِ منْ تجاربِ التعلّمِ المخصصةِ، إلى أنظمةِ التدريسِ الذكيةِ؛ إذْ يُحدثُ الذكاءُ الاصطناعيُّ ثورةً في طريقةِ تعليمِنا وتعلُّمِنا.

لنستعرضْ أهمَّ الخدماتِ التي يقدمُها الذكاءُ الاصطناعيُّ لقطاعِ التعليمِ:

التعلّمُ المخصَّصُ

يمكنُ للذكاءِ الاصطناعيِّ أنْ يساعدَ المعلمينَ في توفيرِ الوقتِ، وتبسيطِ العمليةِ التعليميةِ عنْ طريقِ توفيرِ أدواتٍ لإنشاءِ المحتوى التعليميِّ الذي يتناسبُ وحاجاتِ الطلبةِ وقدراتِهم. بالإضافةِ إلى منصاتِ التعلّمِ المدعومةِ بالذكاءِ الاصطناعيِّ التي تمكّنُ الطلبةَ منْ تلقي محتوًى مخصصٍ وإرشاداتٍ؛ بناءً على احتياجاتِهم وتفضيلاتِهم الفرديةِ.

إنشاءُ محتوًى ذكيٍّ

يُمكِّنُ الذكاءُ الاصطناعيُّ المعلمينَ والطلبةَ منْ إنشاءِ محتوًى تعليميٍّ عالي الجودةِ بمساعدةِ خوارزمياتِ معالجةِ اللغةِ الطبيعيةِ، فيمكنُ للذكاءِ الاصطناعيِّ فحصُ الموادِّ التعليميةِ وتوليدِها بفعاليةٍ بالنصوصِ والصوتِ والصورِ؛ ممَّا يُقلّلُ منَ الجهدِ والوقتِ المطلوبيْنِ لإعدادِهِ. على سبيلِ المثالِ، تساعدُ الأدواتُ التي أُنشِئتْ بوساطةِ الذكاءِ الاصطناعيِّ في إعدادِ الواجباتِ، والاختباراتِ، وخططِ الدروسِ التي تتماشى معَ النتاجاتِ التعليميةِ المحدّدةِ مسبقًا، ويمكنُ لهذهِ الأدواتِ تحليلُ مجموعاتٍ ضخمةٍ منَ البياناتِ، واستخراجُ المعلوماتِ ذاتِ الصلةِ، وتقديمُها بطريقةٍ منظمةٍ ومتسقةٍ.

أنظمةُ التقييمِ الذكيةِ

يمكنُ لأنظمةِ التقييمِ المدعومةِ بالذكاءِ الاصطناعيِّ تحليلُ الواجباتِ والاختباراتِ والأسئلةِ المفتوحةِ للطلبةِ وتقييمُها عنْ طريقِ استخدامِ خوارزمياتِ التعلّمِ الآليِّ؛ إذْ يمكنُ لهذهِ الأنظمةِ تحديدُ الأنماطِ، وتقديمُ تعليقاتٍ متسقةٍ وموثوقةٍ للطلبةِ؛ ممّا يسمحُ للمعلمينَ بالتركيزِ أكثرَ على تقديمِ الإرشادِ والدعمِ الشخصيِّ، بدلًا منْ قضاءِ وقتٍ مفرطٍ في التقييمِ.

الصفوفُ الدراسيةُ الافتراضيةُ والواقعُ الافتراضيُّ

سلطتْ جائحةُ كوفيدَ-19 العالميةُ الضوءَ على الحاجةِ إلى أساليبَ بديلةٍ للتعليمِ؛ حيثُ ظهرتِ الصفوفُ الدراسيةُ الافتراضيةُ المدعومةُ بالذكاءِ الاصطناعيِّ كحلٍّ لسدِّ الفجوةِ بينَ التعليمِ الوجاهيِّ والتعليمِ عنْ بُعدٍ، ويمكنُ للصفوفِ الدراسيةِ الافتراضيةِ المدعومةِ بالذكاءِ الاصطناعيِّ تسهيلُ التعاونِ بينَ الطلبةِ في العملِ على مشروعاتٍ جماعيةٍ، والمشاركةُ في مناقشاتٍ تفاعليةٍ، وتبادلُ الأفكارِ والتعليقاتِ؛ ممّا يُعزّزُ العملَ الجماعيَّ، ومهاراتِ التواصلِ والتعاونَ بينَ الطلبةِ.

أنظمةُ الدعمِ الطلابيِّ الذكيةِ

تؤدي أنظمةُ دعمِ الطلبةِ دورًا مهمًا في تقديمِ الدعمِ التعليميِّ والاجتماعيِّ للطلبةِ، ويساعدُ الذكاءُ الاصطناعيُّ في توفيرِ الدعمِ المستمرِ للطلبةِ على مدارِ الساعةِ، وتقييمِ مشكلاتهم

نشاط عملي

أســـتخدمُ أحدَ برامجَ الذكاءِ الاصطناعيِّ التوليديِّ مثلَ (ChatGPT أو Bing AI) لكتابةِ نصٍّ مكوّنٍ منْ ثلاثِ فقراتٍ عنْ أهميةِ الذكاءِ الاصطناعيِّ في التعليمِ لكلٍّ منَ المعلمينَ والطلبةِ.

بعدَ الانتهاءِ، أُجيبُ عنِ الأسئلةِ الآتيةِ:

- ما السؤالُ أوِ الجملةُ التي كتبتُها في البرنامجِ للحصولِ على النصِّ المطلوبِ؟
- هلْ كانَ النصُّ الذي تمَّ توليدُهُ كافيًا ويحقّقُ المطلوبَ؟
- ما الذي يمكنُ إضافتُهُ أوْ تغييرهُ في الجملةِ للحصولِ على نصٍّ أكثرَ دقةً؟

ثمَّ:

- أعيدُ كتابةَ الجملةِ بشكلٍ أكثرَ تحديدًا.
- ألاحظُ إذا ما تغيّرَ النصُّ المولَّدُ، وأفسرُ السببَ.
- أحفظُ النصَّ المولَّدَ في ملفِ Word على جهازي.

بعدَ ذلكَ، أقارنُ النصَّ الذي حصلتُ عليهِ معَ نصوصِ زملائي، ثمَّ أُناقشُ معَهم أيَّ النصوصِ كانَ أكثرَ شموليةً.

أناقش

دراســـةُ الإيجابياتِ والتحدياتِ الناتجةِ عنِ اســـتخدامِ أدواتِ الذكاءِ الاصطناعيِّ في إنشاءِ المحتوى

أبحثُ في الفوائدِ والتحدياتِ المتعلقةِ باستخدامِ أدواتِ الذكاءِ الاصطناعيِّ لإنشاءِ المحتوى، ثمَّ ألخِّصُ أهمَّ النقاطِ التي توصلتُ إليها، وأُشاركُها معَ المجموعاتِ الأخرى للنقاشِ وتبادلِ الأفكارِ.

نشاط فردي

استكشافُ برامجِ الفصولِ الافتراضيةِ

أذكرُ اسمَ تطبيقٍ للفصولِ الافتراضيةِ استخدمتُهُ وعملتُ عليهِ مسبقًا، ثمَّ أبحثُ عنْ أسماءِ برامجَ أُخرى للفصولِ الافتراضيةِ عنْ طريقِ المصادرِ الموثوقةِ المتاحةِ. بعدَ جمعِ المعلوماتِ، أُشاركُ قائمةَ هذهِ البرامجِ على اللوحِ التفاعليِّ الرَّقميِّ للصفِّ.

إضاءةٌ

بينما تقدمُ تطبيقاتُ الذكاءِ الاصطناعيِّ في التعليمِ إمكاناتٍ كبيرةً، هناكَ أيضًا اعتباراتٌ أخلاقيةٌ وتحدياتٌ تحتاجُ إلى معالجةٍ، وتُعدُّ خصوصيةُ البياناتِ، والتحيّزُ الخوارزميُّ، والحاجةُ إلى التدخّلِ البشريِّ منْ بينِ المخاوفِ الرئيسةِ التي يجبُ أخذُها بعينِ الاعتبارِ عندَ تنفيذِ الذكاءِ الاصطناعيِّ في التعليمِ؛ لذا منَ الضروريِّ وضعُ سياساتٍ قويةٍ لخصوصيةِ البياناتِ، وضمانُ الامتثالِ للوائحِ ذاتِ الصلةِ لحمايةِ المعلوماتِ الحساسةِ للطلبةِ. بالإضافةِ إلى الخوفِ منِ اعتمادِ الطلبةِ بشكلٍ كليٍّ على تطبيقاتِ الذكاءِ الاصطناعيِّ في حلِّ الواجباتِ والأنشطةِ؛ مما يؤثرُ في دقةِ التقييمِ وصدقِهِ.

الرعايةُ الصحيةُ (Healthcare)

يبينُ الشّكلُ (2- 1) فوائدَ استخدامِ الذكاءِ الاصطناعيِّ في الرعايةِ الصحيةِ.

وفي ما يأتي توضيحٌ لبعضٍ منها:

الشّكلُ (2-1): فوائدُ تطبيقاتِ الذكاءِ الاصطناعيِّ في الرعايةِ الصحيةِ

- **تحليلُ البياناتِ الطبيةِ:** تساعدُ أدواتُ الذكاءِ الاصطناعيِّ في تحليلِ البياناتِ الطبيةِ الفرديةِ للمرضى، بما في ذلكَ التاريخُ الطبيُّ، والمعلوماتُ الجينيةُ، وعواملُ نمطِ الحياةِ؛ ممّا يمكّنُ خوارزمياتُ الذكاءِ الاصطناعيِّ منْ توليدِ توصياتٍ علاجيةٍ مخصّصةٍ تأخذُ في الاعتبارِ

الخصائصَ الفريدةَ لكلِّ مريضٍ، وتساعدُ في تحسينِ نتائجِ العلاجِ وتقليلِ الآثارِ السلبيةِ.

- **معالجةُ الصورِ الطبيةِ:** يمكنُ باستخدامِ الذكاءِ الاصطناعيِّ معالجةُ صورِ الأشعةِ السينيةِ، والرنينِ المغناطيسيِّ، والتصويرِ المقطعيِّ، لاكتشافِ الشذوذاتِ الدقيقةِ التي قدْ تفوِّتها عيونُ البشرِ؛ ممّا يؤدي إلى الكشفِ المبكّرِ عنْ حالاتٍ مرضيةٍ صعبةٍ، مثلَ السرطانِ، وأمراضِ القلبِ والأوعيةِ الدمويةِ، والاضطراباتِ العصبيةِ، ويتيحُ أيضًا إجراءَ التدخلاتِ في الوقتِ المناسبِ.
- **الجراحةُ:** يمكنُ استخدامُ المساعداتِ الروبوتيةِ التي يُتَحكَّمُ فيها بوساطةِ خوارزمياتِ الذكاءِ الاصطناعيِّ، بالتعاونِ معَ الجراحينَ البشريينَ لتعزيزِ الدقةِ في العملياتِ الجراحيةِ، وتوفّرُ هذهِ الأنظمةُ مرونةً وثباتًا أكبرَ في الإجراءاتِ الجراحيةِ المعقدةِ معَ تحسينِ الدقةِ.
- **الاستكشافُ في البيئاتِ الخطيرةِ:** يسهمُ الذكاءُ الاصطناعيُّ في تسريعِ عمليةِ اكتشافِ الأدويةِ عنْ طريقِ تحليلِ كمياتٍ ضخمةٍ منَ البياناتِ البيولوجيةِ والكيميائيةِ؛ لتحديدِ المُركّباتِ الأكثرِ فعاليةً ضدَ الأمراضِ المستهدفةِ.

نشاط عملي

أبحثُ وأُناقشُ

أبحثُ في أحدِ تطبيقاتِ الذكاءِ الاصطناعيِّ المتعلقةِ بالتشخيصِ الطبيِّ، مثلَ (مشخّصِ الأمراضِ الجلديةِ في جوجل (DermAssist)، وصحتي(Sohati.com)، وويب طبّ (Webteb.com) ثمَّ أستخدمُها للتعرّفِ إلى حالةٍ مرضيةٍ لها أعراضٌ محددةٌ.

أناقشُ أفرادَ مجموعتي في الأسئلةِ الآتيةِ، ثمَّ أُشاركُ ما نتوصلُ إليهِ معَ بقيةِ المجموعاتِ:

- ما مصداقيةُ المعلوماتِ التي حصلتَ عليها، وما مدى دقتِها؟
- هلْ يمكنُ أنْ تُغْنِيَ هذهِ التطبيقاتُ عنْ زيارةِ الطبيبِ؟ أُفسرُ إجابتي.
- هلْ يمكنُ أنْ تساعدني هذهِ التطبيقاتُ في الاكتشافِ المبكرِ لبعضِ الأمراضِ، وتُسرِّعَ في زيارتي للطبيبِ المختصِّ؟

الأعمالُ التجاريةُ (Retail)

تسعى القطاعاتُ التجاريةُ المختلفةُ إلى التقدمِ عنْ طريقِ تحسينِ الكفاءةِ، وتوفيرِ تجاربَ مخصصةٍ للعملاءِ، وتعزيزِ استراتيجياتِ التسويقِ، وقدْ أحدثَ الذكاءُ الاصطناعيُّ ثورةً في المجالِ التجاريِّ ضمنَ هذهِ الأهدافِ. يبيّنُ الشّكلَ (2– 2) بعضَ فوائدِ الذكاءِ الاصطناعيِّ في التجارةِ.

الشكل (2–2): فوائد الذكاء الاصطناعي في الأعمال التجارية

في ما يأتي بعضُ التطبيقاتِ المهمةِ للذكاءِ الاصطناعيِّ في مجالِ الأعمالِ:

- **تحليلُ بياناتِ العملاءِ**: تُستخدمُ تِقْنيّاتُ التعلّمِ الآليِّ لتحليلِ بياناتِ العملاءِ وتقديمِ توصياتٍ مخصصةٍ؛ ممّا يساعدُ الشركاتِ في تحسينِ تجربةِ التسوّقِ وزيادةِ المبيعاتِ. على سبيلِ المثالِ، تَستخدمُ شركاتٌ مثلَ Amazon خوارزمياتِ الذكاءِ الاصطناعيِّ؛ لتقديمِ توصياتٍ مخصّصةٍ؛ بناءً على تاريخِ الشراءِ وسلوكِ المستخدمِ.
- **التحليلُ التنبؤيُّ**: يعتمدُ التحليلُ التنبؤيُّ على استخدامِ تِقْنيّاتٍ متقدمةٍ مثلَ التعلّمِ الآليِّ، والنماذجِ الإحصائيةِ، والتعلّمِ العميقِ لتحليلِ البياناتِ، وتحديدِ الأنماطِ والعلاقاتِ التي يمكنُ أنْ تساعدَ في التنبؤِ بالأحداثِ المستقبليةِ أوْ سلوكِ العملاءِ، أوِ الأداءِ بناءً على البياناتِ التاريخيةِ؛ ممّا يساعدُ في اتخاذِ قراراتٍ مدروسةٍ وإدارةِ المخزونِ بفعاليةٍ.
- **أدواتُ الدردشةِ الذكيةِ (Chatbots)**: تسهمُ هذهِ الأدواتُ في تحسينِ خدمةِ العملاءِ عنْ طريقِ توفيرِ دعمٍ فوريٍّ وفعّالٍ على مدارِ الساعةِ، ممّا يُقلّلُ منَ التكاليفِ التشغيليةِ ويحسّنُ رضا العملاءِ

إثراء

ذكاءُ الأعمـــالِ (Business Intelligence) هوَ مجموعةٌ منَ العملياتِ والتِّقْنيّاتِ والأدواتِ التي تتيحُ للمؤسساتِ والشركاتِ جمعَ البياناتِ منْ أنشطتِها وأعمالِها المختلفةِ وتحليلَها؛ بهدفِ اتخاذِ قراراتٍ مدروسةٍ ومبنيةٍ على معلوماتٍ دقيقةٍ وموثوقةٍ، ويعتمدُ ذكاءُ الأعمالِ بشكلٍ كبيرٍ على تِقْنيّاتِ الذكاءِ الاصطناعيِّ لبنائِها، ويعدُّ تطبيقُ PowerBI منْ شـــركةِ ميكروسوفت أحدَ الأمثلةِ على أدواتِ تحليلِ البياناتِ وتصويرِها.

إضاءةٌ

أظهرتْ دراســـةٌ قامتْ بها شركةُ ميكروسوفت في الشرقِ الأوســـطِ وإفريقيا شملتْ 112 مؤسسةً، وغطّتْ سبعةَ قطاعاتٍ رئيسةٍ -منها الصحةُ والتصنيعُ والمواردُ والخدماتُ الماليةُ والخدماتُ المِهْنيةُ وتجـــارةُ التجزئةِ والاتصالاتُ وتكنولوجيا المعلوماتِ والإعلامُ والبنيةُ التحتيةُ والنقلُ- أنَّ ما يقاربُ منْ نصفِ الشركاتِ الأردنيةِ تُصنفُ الذكاءَ الاصطناعيَّ أولويةً رقميةً، وبينتْ وزارةُ الاقتصادِ الرَّقْميِّ والريادةِ وجودَ شركاتٍ ناشئةٍ أردنيةٍ تبنتْ حلولًا تِقْنيّةً مبنيةً على الذكاءِ الاصطناعيِّ، مثلَ شـــركةِ **موضوع** التي أطلقتْ أوّلَ مساعدٍ إلكترونيٍّ ناطقٍ باللغةِ العربيةِ مبنيٍّ على الذكاءِ الاصطناعيِّ.

نشاط فردي

أبحثُ في تطبيقاتِ تِقْنيّةِ الذكاءِ الاصطناعيِّ في الأعمالِ التجاريةِ في الأردنِّ وأُشاركها معَ زملائي في الصفِّ.

الصناعةُ (Industry)

أسهمَ الذكاءُ الاصطناعيُّ بدفعِ الابتكارِ وزيادةِ الكفاءةِ في الصناعةِ؛ ممّا يساعدُ في تحقيقِ أداءٍ عالٍ وتنافسيةٍ قويةٍ. ومنْ أبرزِ تطبيقاتِ الذكاءِ الاصطناعيِّ في هذا المجالِ:

- **تحليلُ البياناتِ والتنبؤُ بالمشـــكلاتِ**: استُخدمتْ خوارزمياتُ التعلّمِ الآليِّ لتحليلِ بياناتِ المعداتِ والتنبؤِ بالمشكلاتِ قبلَ حدوثِها؛ ممّا ساعدَ في تجنّبِ الأعطالِ المكلفةِ، وتحسينِ استمراريةِ التشغيلِ. بالإضافةِ إلى تحليلِ بياناتِ الطلبِ والتوريدِ بشـــكلٍ فعّالٍ، وقد ساعدَ هذا الشركاتِ على تحسينِ مستوياتِ المخزونِ وتلبيةِ احتياجاتِ السوقِ بشكلٍ أسرعَ.
- **الأتمتةُ الذكيةُ**: يعززُ الـــذكاءُ الاصطناعيُّ منْ فعاليةِ عملياتِ التصنيعِ؛ حيثُ تُســـتخدمُ الروبوتاتُ الصناعيةُ المدعومةُ بالذكاءِ الاصطناعيِّ لتنفيذِ مهامَّ معقدةٍ بدقةٍ وسرعةٍ؛ ممّا يُقلّلُ منَ الخطأِ البشريِّ، ويزيدُ منْ جودةِ المنتجاتِ.

أبحث

أبحثُ باستخدام (Bing AI) عنْ تطبيقاتٍ أُخرى للذكاءِ الاصطناعيِّ في الصناعةِ، ثمَّ أستخدمُ تطبيقَ الذكاءِ الاصطناعيِّ (Fotor) لإنتاجِ صورٍ متعلقةٍ بالموضوعِ بعدَ وصفِها وصفًا دقيقًا، وأنظِّمُها في مستندِ (Google Docs)، وأشاركهُ على اللوحِ التفاعليِّ الرَّقْميِّ للصفِّ.

الأمنُ السيبرانيُّ (Cyber Security)

تُعدُّ مسألةُ الأمنِ السيبرانيِّ واحدةً منْ أبرزِ التحدياتِ التي تواجهُ المؤسساتِ في عصرِنا الحديثِ، وقدْ أصبحَ استخدامُ الذكاءِ الاصطناعيِّ في هذا المجالِ ضرورةً لا غنى عنها لتعزيزِ الأمانِ، والحمايةِ منَ التهديداتِ المتزايدةِ.

في ما يأتي بعضُ التطبيقاتِ الرئيسةِ للذكاءِ الاصطناعيِّ في الأمنِ السيبرانيِّ:

- **تحليلُ البياناتِ واكتشافُ الأنشطةِ غيرِ الطبيعيةِ أوِ المشبوهةِ:** تُسهمُ تِقْنيّاتُ الذكاءِ الاصطناعيِّ بشكلٍ فعّالٍ في اكتشافِ التهديداتِ السيبرانيةِ ومنعِها عنْ طريقِ مراقبةِ حركةِ مرورِ الشبكةِ، وسجلاتِ النظامِ، وسلوكِ المستخدمِ بشكلٍ مستمرٍ. والقدرةُ على تحليلِ البياناتِ بشكلٍ معمّقٍ، تمكّنُ منَ التعرّفِ إلى أيِّ علاماتٍ تدلُّ على نشاطٍ ضارٍّ مثلَ البرمجياتِ الخبيثةِ والاختراقاتِ. .
- **أتمتةُ عملياتِ الاستجابةِ للحوادثِ:** خوارزمياتُ الذكاءِ الاصطناعيِّ قادرةٌ على اكتشافِ الشذوذِ في سلوكِ الشبكةِ أوْ نشاطِ المستخدمِ؛ ممّا قدْ يشيرُ إلى هجماتٍ غيرِ مرئيةٍ مسبقًا، أوْ محاولاتِ اختراقٍ متقدمةٍ، ويتيحُ هذا النهجُ للمؤسساتِ الاستجابةَ بسرعةٍ لحوادثِ الأمانِ؛ ممّا يُقلّلُ منْ زمنِ الاستجابةِ، ويحدُّ منَ الأضرارِ الناتجةِ عنِ الهجماتِ السيبرانيةِ.
- **أنظمةُ الأمانِ المتقدمةِ:** نظرًا إلى أنَّ مجرمي الإنترنت يطورونَ تِقْنيّاتِهمْ واستراتيجياتِهمْ باستمرارٍ، فمنَ الضروريِّ أنْ تظلَ أنظمةُ الأمانِ متطورةً، ويمكنُ لأنظمةِ الذكاءِ الاصطناعيِّ التدربُ على مجموعةِ بياناتٍ محدّثةٍ باستمرارٍ، تتضمنُ معلوماتٍ حولَ التهديداتِ الناشئةِ، ونقاطِ الهجومِ المتطورةِ، وتحليلِ هذهِ البياناتِ؛ للتعرّفِ إلى أنماطٍ جديدةٍ ومؤشراتٍ على الاختراقِ؛ ممّا يمكّنُ منَ اكتشافِ التهديداتِ السيبرانيةِ غيرِ المعروفةِ مسبقًا وتخفيفِها، وهذهِ القدرةُ التكيُّفيةُ تعززُ منْ مرونةِ دفاعاتِ الأمنِ السيبرانيِّ، وتُقلّلُ منْ خطرِ الهجماتِ الناجحةِ.

نشاط جماعي

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنْ مواقعَ للأمنِ السيبرانيِّ تستخدمُ تطبيقاتِ الذكاءِ الاصطناعيِّ، ثمَّ أستكشفُها لمعرفةِ خصائصِها وميزاتِها، وأشاركُها على اللوحِ التفاعليِّ الرَّقْميِّ للصفِّ.

نشاط فردي

أبحثُ عنْ مؤسساتٍ أردنيةٍ وإقليميةٍ توظفُ الذكاءَ الاصطناعيِّ، معَ ذكرِ مجالِ عملِ الشركةِ والقطاعِ المستهدفِ لمنتجاتِها، ثمَّ أستخدمُ تِقْنيّةَ الكتابةِ بالصوتِ (Voice Typing) منْ أدواتِ تطبيقِ مستنداتِ جوجل (Google Docs)؛ لقراءةِ ما توصلتُ إليهِ، ثمَّ أُدقّقُ النصَّ المكتوبَ الذي ولَّدَهُ التطبيقُ وأحفظُهُ، ثمَّ أناقشُ زملائي في المجموعةِ بالتحدياتِ التي واجهتْني، وكيفَ تغلّبتُ عليها، وأُشاركُ تجربَتي معَ زملائي في الصفِّ.

نشاط فردي

أبحثُ عنْ قطاعاتٍ أُخرى تُذْكَرُ في الدرسِ، وأذكرُ دورَ الذكاءِ الاصطناعيِّ في تحسينِها، والمستقبلَ المتوقعَ لها معَ تِقْنيّاتِ الذكاءِ الاصطناعيِّ، ثمَّ أستخدمُ أحدَ تطبيقاتِ الذكاءِ الاصطناعيِّ في إعدادِ العروضِ التقديميةِ لإعدادِ عرضٍ تقديميٍّ، ومشاركتِهِ عبرَ اللوحِ الرَّقْميِّ التفاعليِّ للصفِّ.

إثراء

قرَّر مجلس الوزراء الموافقة على "الميثاق الوطني لأخلاقيات الذَّكاء الاصطناعي" وتعميمه على جميع الوزارات والمؤسَّسات والدَّوائر الحكوميَّة للالتزام بما ورد فيه حسب الأصول.

ويهدف الميثاق إلى التأكيد على إيجاد قاعدة أخلاقيَّة مشتركة، تنظِّم تطوير تقنيَّات الذّكاء الاصطناعي التي تنبع من القيم الإنسانيَّة والدينيَّة وعادات المجتمع وتقاليده، ورفع الوعي بالمخاطر التي يمكن أن تنتج عن الممارسات الخارجة عن الإطار الأخلاقي المسؤول والآمن.

ويتضمَّن الميثاق مجموعة من المبادئ الأخلاقيَّة الأساسيَّة التي تشمل: قابليَّة المساءلة والشَّفافيَّة، وعدم التحيُّز، ومراعاة الخصوصيَّة، وتعزيز القيم الإنسانيَّة وغيرها من المبادئ التي تعزِّز سيادة القانون وحقوق الإنسان والقيم الدِّيمقراطيَّة والتَّنوُّع، وتراعي أهمَّ المسائل الأخلاقيَّة لاستخدام الذَّكاء الاصطناعي، مع مراعاة متطلَّبات الابتكار والإبداع وحماية حقوق الملكيَّة الفكريَّة. وللاطلاع على بنود الميثاق امسح الرمز سريع الاستجابة المجاور.

المُواطَنةُ الرَّقْميةُ

- **السلامةَ والأمانَ والأمنَ السيبرانيَّ**: يجبُ التأكدُ منْ حمايةِ تطبيقاتِ الذكاءِ الاصطناعيِّ منَ التهديداتِ السيبرانيةِ، مثلَ القرصنةِ أوِ الهجماتِ الإلكترونيةِ، واستخدامِ تِقْنيّاتِ تشفيرٍ حديثةٍ وآلياتِ حمايةٍ قويةٍ.
- **النزاهةَ الرَّقْميةَ**: عندَ استخدامِ الذكاءِ الاصطناعيِّ في مجالاتٍ حساسةٍ، مثلَ الطبِ أوِ السياراتِ الذاتيةِ القيادةِ، يجبُ التأكدُ منْ سلامةِ النظامِ واختبارِهِ بدقةٍ؛ لضمانِ تجنُّبِ الحوادثِ والأخطاءِ.
- **الاحترامَ عبرَ الإنترنت**: يمكنُ أنْ يساعدَ الذكاءُ الاصطناعيُّ في تسهيلِ التواصلِ؛ لكنْ منَ المهمِ التأكدُ منْ أنَّ الأدواتِ المستخدمةَ، لا تنتهكُ قواعدَ الاحترامِ والتواصلِ البنّاءِ عبرَ الإنترنت.

مشروع

المشروعُ: إنتاجُ سلسلةٍ منْ مقاطعِ الفيديو التعليميةِ (الرسومِ المتحركةِ) على شكلِ حلْقاتٍ؛ حيثُ تتناولُ كلُّ حلْقةٍ موضوعًا محددًا، باستخدامِ تطبيقاتِ الذكاءِ الاصطناعيِّ / المهمةُ2.

أُكملُ معَ زملائي سلسلةَ الحلْقاتِ التعليميةِ (الرسومِ المتحركةِ) بتنفيذِ الخطواتِ الآتيةِ:

- إعدادُ السيناريوهاتِ التعليميةِ للحلْقةِ الثانيةِ؛ بحيثُ تشملُ تحديدَ الشخصياتِ، والحوارَ المكتوبَ والمسموعَ، والخلفياتِ، والتسلسلَ البصريَّ للمشاهدِ، وتُستخدمُ كمرجعٍ أساسيٍّ في أثناءِ إنتاجِ الفيديوهاتِ.
- إنتاجُ الحلْقةِ الثانيةِ؛ بناءً على السيناريوهاتِ المكتوبةِ التي تتحدثُ عنْ ثلاثةٍ منْ مجالاتِ استخداماتِ الذكاءِ الاصطناعيِّ الآتيةِ، معَ تضمينِ إنجازاتٍ محليةٍ وعربيةٍ وعالميةٍ في التعليمِ، والرعايةِ الصحيةِ، والأعمالِ التجاريةِ، والصناعةِ، والأمنِ السيبرانيِّ، والنقلِ، والزراعةِ، والبحثِ العلميِّ.
- أستخدمُ تطبيقاتِ الذكاءِ الاصطناعيِّ الواردةِ في المهمةِ الأولى.
- **أُراعي عندَ إعدادِ الحلْقاتِ التعليميةِ ما يأتي:**
  - دقةَ المعلوماتِ وحداثتُها.
  - مناسبةَ وقتِ الفيديو (الحلْقةِ التعليميةِ) معَ الموضوعِ.
  - التشويقَ والجاذبيةَ.
  - التسلسلَ المنطقيَّ لعرضِ المحتوى.
  - التوثيقَ للمراجعِ والمصادرِ ونواتجَ عملِ المجموعاتِ.

أقيِّمُ تعلّمي

المعارفُ: أُوظفُ في هذا الدرسِ ما تعلمتُهُ منْ معارفَ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأوّلُ: أوضحُ المقصودَ بالمصطلحاتِ الآتيةِ: التعلّمِ المخصّصِ، أنظمةِ التقييمِ الذكيةِ.

.....

السـؤالُ الثاني: أُبينُ أربعةَ مجالاتٍ أسـتخدِمُ فيها الذكاءَ الاصطناعيَّ، معَ ذكرِ فائدةٍ تحققتْ منِ استخدامي لكلٍّ منها.

.....

المهاراتُ: أُوظفُ مهاراتِ التفكيرِ الناقدِ، والتواصلِ الرَّقْميِّ، والبحثِ الرَّقْميِّ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السـؤالُ الأوّلُ: هلْ تعتقدُ أنْ الذكاءَ الاصطناعيَّ يمكنُ أنْ يحلَّ محلَّ الأطباءِ في المستقبلِ؟ أفسرُ إجابتي، ثمَّ أبحثُ عنِ الموضوعِ في المصادرِ الموثوقةِ.

.....

السؤالُ الثاني: كيفَ يمكنُ تطبيقُ تِقْنيّاتِ الذكاءِ الاصطناعيِّ في مجالِ السياحةِ؟

.....

السؤالُ الثالثُ: ما تِقْنيّاتُ الذكاءِ الاصطناعيِّ التي تُوظَّفُ في السياراتِ ذاتيةِ القيادةِ؟

.....

السؤالُ الرابعُ: أُقدمُ مقترحاتٍ في كيفيةِ توظيفِ الذكاءِ الاصطناعيِّ لحلِّ أزمةِ الغذاءِ العالميةِ.

.....

السـؤالُ الخامسُ: أُفكرُ في تِقْنيّاتِ الذكاءِ الاصطناعيِّ التي يمكنُ استخدامُها لتحسينِ التنبؤاتِ الجويةِ.

.....

القيمُ والاتجاهاتُ:

أُصممُ ملصقًا باسـتخدامِ أحدِ تطبيقاتِ الذكاءِ الاصطناعيِّ في التصميمِ عنِ الاستخدامِ المسؤولِ لتطبيقاتِ الذكاءِ الاصطناعيِّ، ثمَّ أُشاركُه معَ زملائي/ زميلاتي في المدرسةِ.

الدرسُ الثالثُ

الروبوتُ (Robot)

الفكرةُ الرئيسةُ:

التعرُّفُ إلى الروبوتاتِ، ومكوناتِها، وأنواعِها، واستخداماتِها، وأهميتِها.

المفاهيمُ والمصطلحاتُ:

الروبوتُ (Robot)،

الحسّاساتُ (Sensors)،

الروبوتاتُ على هيئةِ إنسانٍ – الرجلُ الآليُّ (Anthropomorphic Robots)،

المحركاتُ (Motors)،

الروبوتات المجسمةُ (Anthropomorphic Robots)،

الروبوتُ على هيئةِ ذراعٍ (Manipulators)،

طائراتُ درون (Drones).

نتاجاتُ التعلّمِ (Learning Outcomes)

- أتعرَّفُ نظامَ الروبوتِ.
- أشرحُ مكوناتِ نظامِ الروبوتِ.
- أوضحُ أهميةَ نظامِ الروبوتِ.
- أذكرُ استخداماتِ الروبوتِ.

منتجاتُ التعلّمِ (Learning Products)

إعدادُ لوحةٍ قصصيةٍ (Storyboards) تفصيليةٍ أساسيةٍ للحلْقةِ الثالثةِ الخاصةِ بالروبوتِ، وإنتاجُ الحلْقةِ باستخدامِ مواقعَ وتطبيقاتِ الذكاءِ الاصطناعيِّ.

نشاط تمهيدي

تخيَّلْ لوِ استُخدمتِ الروبوتاتُ لتقديمِ الرعايةِ للمرضى خلالَ جائحةِ كورونا، بدلًا منَ التعاملِ المباشرِ منْ قبلِ العاملينَ في القطاعِ الصحيِّ، الذينَ تعرّضَ كثيرٌ منهم للخطرِ والوفاةِ نتيجةً لذلكَ. فكّرْ في الفوائدِ والإيجابياتِ التي كانَ يمكنُ أنْ تنتجَ عنِ استخدامِ الروبوتاتِ في هذهِ الأزمةِ الصحيةِ، وكذلكَ السلبياتُ المحتملةُ.

أُشاركُ أفكاري معَ زملائي في الصفِّ، وأُناقشُ معَهم وجهاتِ النظرِ المختلفةِ لاكتسابِ فهمٍ أعمقَ للموضوعِ.

في الماضي، كانتِ الروبوتاتُ تُبنى للقيامِ بمهامَّ لا يستطيعُ الإنسانُ تنفيذها، إما بسببِ صعوبتِها أوْ خطورتِها. معَ ذلكَ، شهدتْ تكنولوجيا الروبوتاتِ تطورًا كبيرًا في الآونةِ الأخيرةِ؛ حيثُ لمْ يعدِ استخدامُها محصورًا في المهامِّ الخطرةِ أوِ الصعبةِ فحسبُ، بلْ توسّعَ ليشملَ جوانبَ متعددةً منَ الحياةِ اليوميةِ، حتى تلكَ الروتينيةِ أوِ المملةِ. واليومُ، تُستخدمُ الروبوتاتُ لتسهيلِ الحياةِ وتمكينِ الأفرادِ، ممّنْ لمْ يكونوا قادرينَ على القيامِ ببعضِ الأعمالِ بأنفسِهمْ، وتحقيقِ درجةٍ منَ الاستقلاليةِ. فما هيَ الروبوتاتُ؟ وما هيَ مكوناتُها وأنواعُها؟ وما أهميتُها؟ وفي أيِّ مجالاتٍ يمكنُ استخدامُها؟

مفهومُ الروبوتِ

يُعرَفُ الروبوتُ بأنّهُ آلةٌ (إلكترو-ميكانيكيةٌ) تبرمَجُ بوساطةِ برامجَ حاسوبيةٍ خاصةٍ مزودةٍ بمحركاتٍ تساعدُهُ على الحركةِ مثلَ أرجلٍ، أوْ عجلاتٍ، أوْ مفاصلَ، أوْ مقابضَ تؤدي مهامَّ محددةً، وتتمكنُ منَ التأثيرِ في البيئةِ الماديةِ، ويُستخدمُ للقيامِ بالعديدِ منَ الأعمالِ الخطرةِ والشاقةِ والدقيقةِ.

ويوصفُ عِلْمُ الروبوتاتِ بأنهُ العلمُ الذي يقومُ علىٰ تصميمِ هذهِ الآلاتِ وبنائِها وبرمجتِها؛ لتتفاعلَ معَ البيئةِ المحيطةِ التي تجمعُ العديدَ منَ المفاهيمِ الخاصةِ بعلمِ الذكاءِ الاصطناعيِّ، منها: الإدراكُ، والتخطيطُ، والتعلّمُ غيرُ الخاضعِ للإشرافِ، والتعلّمُ التعزيزيُّ، وكذلكَ نظريةُ الألعابِ.

مكوناتُ نظامِ الروبوتِ

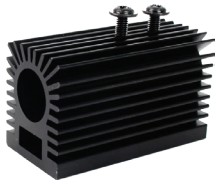
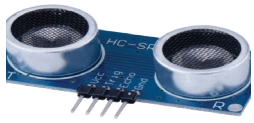
يعملُ الروبوتُ على استقبالِ البياناتِ منَ البيئةِ المحيطةِ، ثمَّ معالجتِها والتصرفِ بها بناءً على هذهِ البياناتِ المَدخلةِ. وتختلفُ مكوناتُ الروبوتِ باختلافِ المهمةِ التي سيؤديها، ولكنْ تتشابَهُ جميعُها بوجودِ مستشعراتٍ ومحركاتٍ ومستجيبٍ نهائيٍّ، وكذلكَ نظامُ التحكمِ. انظرِ الشّكلَ (3-1).

الشكل (3-1): مكونات الروبوت

وفي ما يأتي توضيحٌ لهذهِ المكوّناتِ ولبعضِ المكوناتِ الأخرى التي مِنَ الممكنِ أنْ يُزوَّدَ بها الروبوتُ:

1. **وَحْداتُ الإدخالِ (Input Units)**: يحتاجُ الروبوتُ إلى عددٍ منَ الحسّاساتِ (Sensors) و/أوْ وَحْداتِ الاتصالِ (Communication Modules) مثلَ Wi-Fi وBluetooth بحسبِ مهمتِهِ؛ بهدفِ جمعِ المعلوماتِ منَ البيئةِ المحيطةِ، والتواصلِ وتبادلِ البياناتِ معَ الأجهزةِ الأخرى. يبينُ الجدولُ الآتي بعضَ أنواعِ الحسّاساتِ ومبدأَ عملِها ووظيفتِها:

الجدولُ (3-1): بعضُ أنواعِ الحسّاساتِ ووظيفتُها ومبدأُ عملِها

الحسّاسُ	الوظيفةُ	مبدأُ العملِ	الشّكلُ
الكاميرا (Camera)	الرؤيةُ الحاسوبيةُ	تعتمدُ على الرؤيةِ المجسَّمةِ باستخدامِ كاميراتٍ متعددةٍ؛ بحيثُ يُصوَّرُ الجسمُ منْ زوايا مختلفةٍ، منْ ثمَّ يُحلَّلُ المنظرُ الناتجُ في هذهِ الصورِ للتعرّفِ إلى الأجسامِ المحيطةِ.	
أجهزةُ استشعارِ السونار (Ultrasonic Sensors)	قياسُ المسافةِ	يقيسُ المسافةَ بينَ الروبوتِ والأجسامِ باستخدامِ تِقْنيةِ الأموجِ الصوتيةِ؛ حيثُ يقومُ بإصدارِ هذهِ الموجاتِ وينتظرُ ارتدادَها عنِ الأجسامِ، ويحسبُ المسافةَ اعتمادًا على وقتِ الموجةِ المرتدةِ وكثافتِها.	
حسّاسُ الكاميرا (Kinect Sensor)	الرؤيةُ الحاسوبية	حسّاسٌ رخيصُ الثمنِ نسبيًّا، وهوَ أكثرُ استخدامًا حاليًّا منَ الكاميرا والسونار؛ لأنّهُ يجمعُ بينَ الكاميرا وجهازِ عرضِ الضوءِ المنظمِ (Structured light projector)، ويعملُ على عرضِ نمطٍ معينٍ منَ الخطوطِ على المشهدِ على شكلِ شبكةٍ تعملُ الكاميرا على تحليلِ انحناءاتِ الخطوطِ.	

الحسّاسُ	الوظيفةُ	مبدأُ العملِ	الشّكلُ
حسّاسُ المدى البصريِّ (حسّاسُ الضوءِ) (Optical Range Sensor)	قياسُ المسافةِ	تشبهُ أجهزةَ السونارِ بمبدأِ عملها؛ حيثُ إنّها تصدرُ إشارةً ضوئيةً، وتقيسُ الوقتَ اللازمَ لعودةِ هذهِ الإشارةِ إلى المستشعرِ، منْ ثمَّ حسابُ المسافةِ. تَستخدمُ السياراتُ الذاتيةُ القيادةُ هذا المستشعرَ. يقيسُ هذا الحسّاسُ المسافاتِ منْ 1 سمٍ إلى 100 مترٍ.	
حسّاسُ الليزرِ (LiDAR Sensor)	يستخدم لاستشعار الضوء	لهُ مبدأُ عملِ مستشعرِ الضوءِ نفسِهِ، ولكنْ باختلافِ الإشاراتِ التي يصدرُها.	
حسّاسُ الرادارِ (Radar)	قياسُ المسافاتِ	يقيسُ المسافاتِ أيضًا، ولكنّهُ يستخدمُ الأمواجَ الراديويةَ أوِ (الموجاتِ الكهرومغناطيسيةِ). يُستخدمُ للمركباتِ الجويةِ، حيثُ إنّهُ يقيسُ مسافةً تصلُ إلى كيلو مترات، ويستطيعُ أيضًا العملَ في الضبابِ.	
حسّاسُ الموقعِ (GPS Global Positioning System)	قياسُ الموقعِ	يستطيعُ إرسالَ إشاراتٍ للأقمارِ الصناعيةِ لمعرفةِ الموقعِ بدقةٍ عاليةٍ قدْ تصلُ إلى مليمترٍ في الظروفِ الجيدةِ. لا يُستخدمُ داخلَ المباني أوْ تحتَ الماءِ	
حسّاسُ الصوتِ (Sound Sensor)	يُستخدم للكشف عن الأصوات	يُستخدمُ لاكتشافِ الصوتِ أوِ الاهتزازاتِ الصوتيةِ في مُحيطِهِ؛ بتحويلِ الموجاتِ الصوتيةِ إلى إشاراتٍ كهربائيةٍ يمكنُ قياسُها وتحليلُها.	
حسّاسُ اللمسِ (Touch Sensor)	يستخدم للكشف عن الاجسام المحيطة	يُستخدمُ للكشفِ عنِ اللمسِ أوِ الضغطِ على سطحٍ معينٍ، وتحويلِ هذا التفاعلِ إلى إشارةٍ كهربائيةٍ.	

2. **وَحْـــداتُ المعالجةِ (Processing Units)**: وَحْداتُ المعالجةِ هـــيَ بمنزلةِ العقلِ للروبوتِ، تقومُ بتنفيذِ البرامجِ التي كتبَها المطـــورونَ (Developers) والتي تُحلّلُ البياناتِ الواردةَ منَ المدخلاتِ، واتخاذِ القراراتِ، وإعطاءِ الأوامرِ للمخرجاتِ، وتعدُّ Arduino وRaspberry Pi منَ الأمثلةِ على المعالجاتِ الشائعةِ التي تُبرمَجُ بلغاتٍ برمجةٍ مثلَ Python و C++ وغيرِها منَ اللغاتِ.

3. **وَحْداتُ الإخراجِ (Outputs Units)**: تشـــملُ وحداتُ الإخراجِ كلَّ الأجزاءِ التي تســـتقبلُ الأوامرَ والمعلوماتِ منَ المعالجِ، ويمكنُ تلخيصُ جزءٍ منها كما يأتي:

- **المحركاتُ (Motors)**: هيَ العناصرُ المسؤولةُ عنْ تحويلِ الأوامرِ الكهربائيةِ إلى حركةٍ ميكانيكيةٍ، مثلَ محـــركاتِ DC، ومحركاتِ الســـيرفو (Servo Motors)، والمحركاتِ الخطويةِ (Stepper Motor). تُستخدمُ المحركاتُ لتحريكِ أجزاءِ الروبوتِ، مثلَ العجلاتِ أوِ الأذرعِ.
- **الأذرعُ (Arms)**: هيَ المكوناتُ التي تُســـتخدمُ لتنفيذِ المهامِّ الميكانيكيةِ، مثلَ الالتقاطِ، والتحريكِ، والرفعِ، ويُتحكَّمُ فيها عنْ طريـــقِ المحركاتِ؛ بناءً على الأوامرِ الصادرةِ منْ وَحْدةِ المعالجةِ.
- **العجلاتُ (Wheels)**: تُســـتخدمُ لتحريكِ الروبوتِ في البيئـــاتِ المختلفةِ، والتنقلِ عبرَ التضاريسِ الصعبةِ، مثلَ الرملِ، أوِ الطينِ، أوِ الثلجِ.

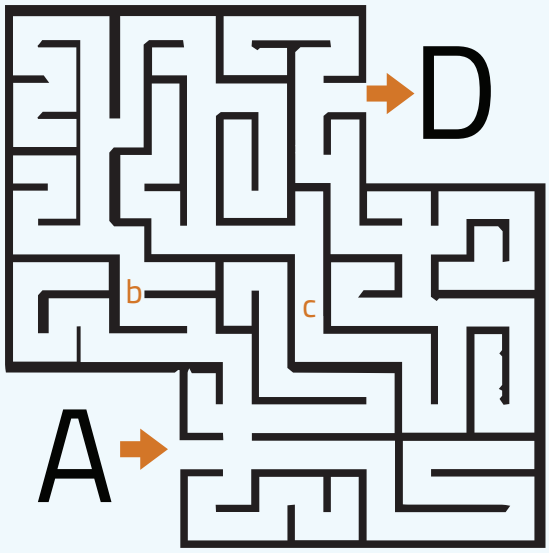
نشاط فردي

استكشافُ وحداتِ الإخراجِ في الروبوتاتِ وتطبيقاتِها

أبحثُ عنْ وحداتِ إخراجٍ أُخرى للروبوتاتِ، وأُحدّدُ كيفَ يمكنُ استخدامُ هذهِ المخرجاتِ في مجالاتٍ متنوعةٍ، وأُشـــاركُ نتائجَ بحثي معَ الزملاءِ عنْ طريـــقِ اللوحِ الرَّقْميِّ التفاعليِّ الخاصِّ بالصفِّ.

نشاط جماعي

أُحللُ وأُناقشُ

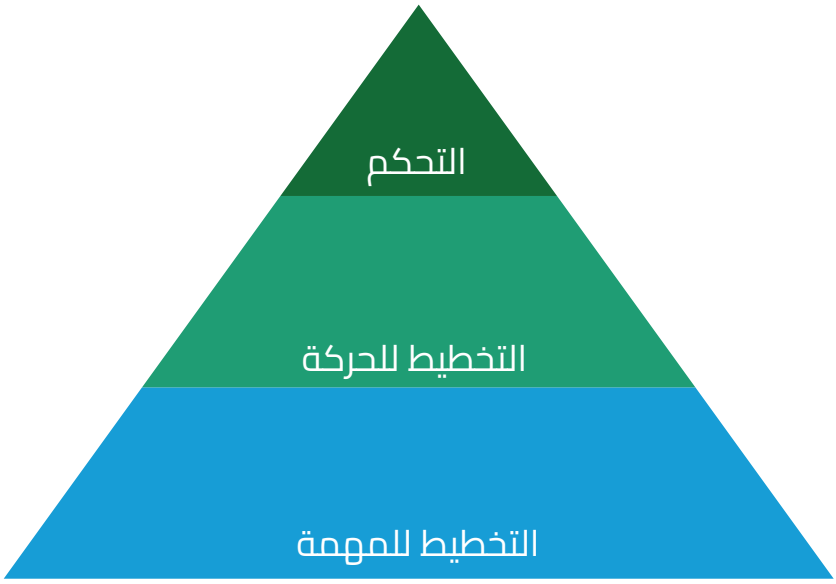


أتأملُ الشـــكلَ المجاورَ، وأصـــفُ بخطواتٍ إجرائيةٍ منظَّمةٍ المسارَ الصحيحَ الذي يجبُ أنْ يسلكهُ الروبوتُ للانتقالِ منَ النقطةِ A إلى النقطةِ D، ثمَّ أصفُ خطواتِ التنفيذِ الإجرائيةِ بشـــكلٍ منظَّمٍ، وأُبينُ الأجزاءَ المستخدمةَ في الروبوتِ لتنفيذِ هذهِ الخطواتِ.

أُناقشُ زملائي في المجموعـــاتِ الأخرى في الأسئلةِ الآتيةِ:

- هلْ توافقتْ إجاباتُ المجموعاتِ في عددِ الخطواتِ وترتيبِها؟
- هلْ يؤثّرُ ترتيبُ الخطواتِ وتنظيمها في تنفيذِ الروبوتِ للمهامِّ؟
- كيفَ تعملُ مكوناتُ الروبوتِ معًا لتنفيذِ المهمةِ بشكلٍ سهلٍ وَمَرنٍ؟

تتحركُ الروبوتاتُ في ثلاثةِ مستوياتٍ هرميةٍ، كما هوَ موضّحٌ في الشّكلِ (3-2):



الشكل (3-2): مستويات حركة الروبوتات

1. **التخطيطُ للمهمَّةِ**: في هذا المستوى يُحدَّدُ هدفُ المهمةِ مثلًا: المهمةُ في النشاطِ السابقِ تتمثلُ في الانتقالِ منَ النقطةِ A إلى النقطةِ D.
2. **التخطيطُ للحركةِ**: في هذا المستوى يُحدَّدُ مسارٌ لنقلِ الروبوتِ أوِ التخطيطِ لتحقيقِ الهدفِ الفرعيِّ.

- المهمةُ الأولى للروبوتِ في هذهِ المرحلةِ، هيَ إدراكُ البيئةِ المحيطةِ عنْ طريقِ تِقْنيةِ الرؤيةِ الحاسوبيةِ. بالإضافةِ إلى الحسّاساتِ التي يمتلكها، وتعدُّ هذهِ العمليةُ صعبةً؛ حيثُ تُعاني الروبوتاتُ أحيانًا منْ مشكلةِ تقديرِ الحالةِ أوِ القدرةِ على فلترةِ التمثيلاتِ الداخليةِ؛ (أيْ ما هوَ مُخزّنٌ داخلَ ذاكرةِ الروبوتِ).

ولتجنبِ هذهِ المشـــكلةِ، يُفضَّلُ أنْ تتوافرَ الخصائصُ الآتيةُ في التمثيلاتِ الداخليةِ للبيئةِ المحيطةِ:

- معلوماتٌ كافيةٌ ليتمكنَ الروبوتُ منِ اتخاذِ القرارِ.
- معلوماتٌ منظَّمةٌ بكفاءةٍ ومحدَّثةٍ بشكلٍ مستمرٍ.
- معلوماتٌ طبيعيةٌ، أيْ أنها تتوافقُ إلى حدٍّ كبيرٍ معَ البيئةِ المحيطةِ.

- تأتي بعدها مهمةُ التحديدِ والتعيينِ، وعندَ الحديثِ عنِ الروبوتاتِ المتحركةِ، فإنها تعني تحديدَ أماكنِ الأشـــياءِ بما فيها الروبوتُ عنْ طريقِ إحداثياتِ المستوى الديكارتيّ، وبُعدِ هذهِ الأشـــياءِ عنِ الروبوتِ، ولكنْ قدْ يواجهُ الروبوتُ مشكلةَ عدمِ وجودِ خريطةٍ للمكانِ أوْ للبيئـــةِ المحيطةِ أصلًا، حينئذٍ يجبُ عليهِ تحديدُ موقعِهِ، مِـــنْ ثَمَّ بناءُ خريطةٍ للمكانِ، وهذهِ العمليةُ تُســـمى بالتوطينِ المتزامنِ (Simultaneous Localization). عندئذٍ تبرزُ قدرةُ الروبوتِ على التعلّمِ الآليِّ منْ دونِ إشرافٍ.
- قدْ يقومُ الروبوتُ بقياسِ درجةِ الحرارةِ أوِ التعرّفِ إلى الصوتِ أوِ الروائحِ، واتخاذِ الإجراءِ المناسبِ إذا بُرمجَ على ذلكَ؛ ولكنْ قدْ يحتاجُ إلى التعلّمِ عنْ طريقِ التكيفِ معَ المتغيراتِ التي لمْ يُبرمجْ عليها، ويُشـــبهُ هذا قدرةَ الســـيارةِ الذاتيةِ القيادةِ على التكيّفِ معَ الطريقِ، ويُسمى هذا أيضًا بالإشرافِ الذاتيِّ.
- تنتهي هذهِ المرحلةُ بتحديدِ الروبوتِ أوِ الجزءِ منَ الروبوتِ المطلوبِ منهُ تحقيقُ الهدفِ في مسارٍ معينٍ، وهذا المسارُ محددٌ بنقاطٍ فرعيةٍ مرتبطةٍ بالزمنِ، مثلًا إذا كانَ على الروبوتِ أنْ يتحركَ منْ نقطةِ A إلى نقطةِ D مرورًا بالنقاطِ b و c وَفْقَ زمنٍ محدّدٍ.

3. **التحكمُ**: هنا تُستخدمُ محركاتُ الروبوتِ لتحقيقِ الحركةِ المخططِ لها، أوِ الهدفِ الفرعيِّ عنْ طريقِ اتّباعِ سلسلةٍ منَ الإجراءاتِ المرتبطةِ بوقتٍ محدّدٍ لكلِّ إجراءٍ.

نشاط فردي

يوّدُ الروبوتُ X تغييرَ المصباحِ الكهربائيِّ، أُفكرُ بالطريقةِ التي يُمكنُ للروبوتِ تغييرُ المصباحِ عنْ طريقها مرورًا بالمستوياتِ الثلاثةِ السابقةِ.

أُحدّدُ الخطواتِ لكلِّ مستوًى، وأبيّنُ كيفَ سيعملُ الروبوتُ في كلٍّ منها.

أستخدمُ أحدَ برامجِ الذكاءِ الاصطناعيِّ لتصميمِ الإنفوجرافيك الذي يعرضُ المستوياتِ الثلاثةِ، وإجراءاتِ الروبوتِ في كلٍّ منها.

أُشاركُهُ زملائي على اللوحِ التفاعليِّ الرَّقْميِّ للصفِّ.

أنواعُ الروبوتاتِ

توجدُ عديدٌ منَ المعاييرِ لتقسيمِ الروبوتاتِ، منها: هيكلةُ الجسمِ. وتُقْسَمُ الروبوتاتُ وفقًا لشكلِها كما يأتي:

- **الروبوتاتُ المجسّمةُ (Anthropomorphic Robots):**

قدْ يأتي على هيئةِ إنسانٍ آليٍّ أوْ هيئةٍ أُخرى، ويتميزُ بأنّهُ يمتلكُ رأسًا ويديْنِ، وَمنَ الممكنِ أنْ يتحركَ هذا الروبوتُ باستخدامِ الأرجلِ أوِ العجلاتِ. ومنَ الأمثلةِ عليهِ الروبوتاتُ في الشّكلِ (3-3).

الشّكلُ (3-3) : بعضُ الأمثلةِ على الروبوتاتِ المجسّمةِ

- **الروبوتُ على هيئةِ ذراعٍ (Manipulators):**

تأخذُ هذهِ الروبوتاتُ شكلَ ذراعٍ كالتي تُثَبَّتُ في المصانعِ، وبعضها تُستخدمُ في تجميعِ السياراتِ، وتُصمَّمُ بحيثُ تستطيعُ حملَ أوزانٍ ثقيلةٍ، والأفضلُ هيَ التي تُثَبَّتُ على الكراسي المتحركةِ؛ لتساعدَ ذوي الإعاقةِ الحركيةِ؛ حيثُ يُتَحكَّمُ بها عنْ طريقِ الصوتِ. انظرِ الشّكلَ (3-4) الذي يبينُ بعضَ هذهِ الأشكالِ.

الشّكلُ (3-4): بعضُ أشكالِ الروبوتِ على هيئةِ ذراعٍ

- **روبوتاتٌ ذواتُ أجنحةٍ:**

منَ الأمثلةِ عليها: الطائراتُ منْ دونِ طيّارٍ رباعيةُ المراوحِ (طائراتُ درون) (Drones) كما يظهرُ في الشّكلِ (3-5).

الشّكلُ (3-5): طائرةُ درون

- **الروبوتُ السبّاحُ (Autonomous Underwater Vehicles: AUVs):**

هيَ روبوتاتٌ تعملُ على استكشافِ أعماقِ المحيطاتِ منْ دونِ تدخلٍ مباشرٍ منَ البشرِ، وتستطيعُ جمعَ بياناتٍ عاليةِ الدقةِ وتخزينَها للاستفادةِ منها في الأبحاثِ العلميةِ. انظرِ الشّكلَ (3-6).

الشّكلُ (3-6): الروبوتُ السبّاحُ

أبحث

استكشافُ الروبوتاتِ المجسَّمةِ

أتعاونُ معَ زملائي في المجموعةِ للبحثِ عنْ أشكالٍ أُخرى منَ الروبوتاتِ المجسَّمةِ، ونبحثُ في أماكنِ استخدامِها ووظائفِها، ثمَّ نعرضُ ما توصلْنا إليهِ أمامَ المجموعاتِ الأخرى، ونتبادلُ الآراءَ والنقاشاتِ معَهم.

نشاط فردي

التفكيرُ في تحويلِ غرفةٍ إلى بيئةٍ روبوتيةٍ ذكيّةٍ

أفكّرُ في تحويلِ غرفتي إلى غرفةٍ روبوتيةٍ، وأتخيلُ أشكالَ الروبوتاتِ التي أحتاج إليها، والفوائدَ المتوقعةَ منِ استخدامها. أسألُ نفسي:

- ما الروبوتاتُ التي ستكونُ جزءًا منْ هذهِ البيئةِ؟
- ما الوظائفُ التي ستقومُ بها هذهِ الروبوتاتُ لتحسينِ حياتي اليوميةِ؟

ثمَّ أفكرُ في التحدياتِ المحتملةِ، مثلَ:

- هلْ ستكونُ الروبوتاتُ معقدةً في التشغيلِ؟
- هلْ ستواجهُ الغرفةُ الروبوتيةُ مشكلاتٍ في التكيّفِ معَ احتياجاتي؟

بعدَ ذلكَ، أستخدمُ أحدَ برامجِ الذكاءِ الاصطناعيِّ للتصميمِ، مثلَ (DALL.E او Fotor)، لوصفِ غرفتي بشكلٍ دقيقٍ، وتحويلِ الوصفِ إلى صورةٍ تُعبّرُ عنْ هذهِ الغرفةِ الذكيةِ.

أشاركُ الصورةَ معَ زملائي، وأناقشُ معَهم مدى مطابقةِ الصورةِ معَ ما تخيلتُهُ، وأسمعُ آراءَهم في تصميمِ الغرفةِ والتحدياتِ المحتملةِ.

نشاط فردي

أتأملُ وأحلّلُ أشكالَ الروبوتاتِ

أتأملُ الأشكالَ المختلفةَ للروبوتاتِ، وأُجيبُ عنِ الأسئلةِ الآتيةِ:

- ما العلاقةُ بينَ شكلِ الروبوتِ ونوعِ الوظيفةِ المبرمجِ عليها؟
- هلْ يُؤثّرُ حجمُ الروبوتِ في سرعةِ أدائهِ ودقتهِ؟

أتخيلُ روبوتًا يمكنُ استخدامُه في الفصلِ، مثلَ المُعلمِ، وأصفهُ وصفًا دقيقًا منْ حيثُ الشّكلُ والوظائفُ.

أستخدمُ أحدَ برامجِ الذكاءِ الاصطناعيِّ مثلَ (Canva ، DALL-E) لتصميمِ ملصقٍ يُعبرُ عنْ شكلِ هذا الروبوتِ المُعلمِ ووظيفتهِ.

أُشاركُ تصميمي معَ زملائي على اللوحِ التفاعليِّ الرَّقْميِّ في الصفِّ، وأُناقشُ معهم أفكارَهم حولَ الروبوتِ التعليميِّ.

مجالاتُ استخدامِ الروبوتِ وأهميتُها

تستخدمُ الروبوتاتُ في مجالاتِ الحياةِ المختلفةِ؛ منْ أجلِ تحقيقِ الاستقلاليةِ، وتحسينِ الخدماتِ الصحيةِ وزيادةِ الإنتاجيةِ.

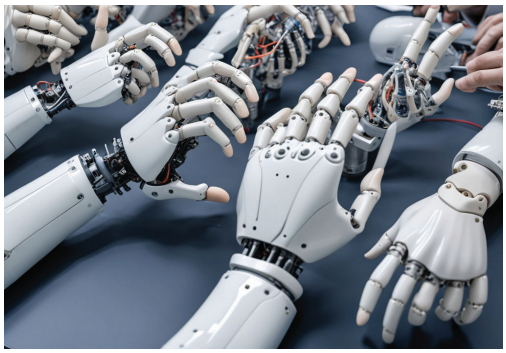
وفي ما يأتي بعضُ الأمثلةِ على استخداماتِ الروبوتِ:

الشّكلُ (3-7): روبوتُ تنظيفِ الأرضياتِ

1. يُستخدمُ الروبوتُ في المنزلِ للعنايةِ بكبارِ السّنِ والأشخاصِ ذوي الإعاقةِ الحركيةِ؛ لتُحقَّقَ لهم الاستقلاليةُ، وتساعدَهم في القيامِ بالمهامِّ. **ومنَ الأمثلةِ على ذلكَ**: ذراعُ الروبوتِ المثبَّتةِ على الكرسي المتحركِ التي تتلقى التعليماتِ الصوتيةَ. ثمَّ إنَّ الباحثين في هذا المجالِ يعملونَ على تطويرِ روبوتٍ يُمكِّنُ المصابينَ بالشللِ الدماغيِّ منَ استخدامِ ذراعٍ روبوتيةٍ للإمساكِ بالأشياءِ، وقدْ تصلُ إلى استخدامِها بما يمكِّنُهم منْ تناولِ الطعامِ بأنفسهِم، وقدْ انتشرَ في الآونةِ الأخيرةِ روبوتٌ يعملُ على تنظيفِ الأرضياتِ كما في الشّكلِ (3-7).

أبحثُ

أبحثُ في المواقعِ الإلكترونيةِ الموثوقةِ عنِ استخداماتٍ أُخرى للروبوتاتِ المنزليةِ، وأُشاركُ ما أتوصلُ إليهِ معَ زملائي في الصفِّ على اللوحِ التفاعليِّ الرَّقْميِّ.

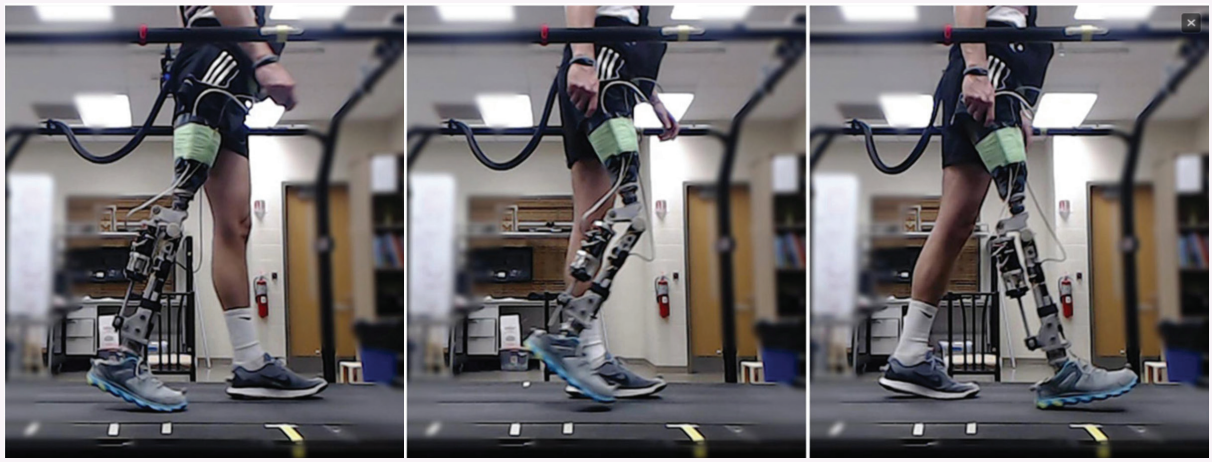


الشكل (3-8): روبوتات أطراف صناعية

2. **المجالُ الطبيُّ**: تُستخدمُ الروبوتاتُ كثيرًا في المجالِ الطبيِّ. وفي ما يأتي بعضُ الأمثلةِ على ذلكَ:

- **الأطرافُ صناعيةُ الروبوتيةِ (Prosthetics)**: يُركَّبُ الطرفُ الصناعيُّ الذكيُّ؛ بحيثُ يرتبطُ بدعائمَ أتوماتيكيةٍ وكهربائيةٍ تتلقى الإشاراتِ منَ الدماغِ، منْ ثمَّ تقومُ بالاستجابةِ لهذهِ الإشاراتِ. ويوضّحُ الشّكلُ (3- 8) بعضًا منْ هذهِ الأطرافِ.

يمثلُ الشّكلُ (3-9) نظامًا لساقٍ صناعيةٍ طُوِّرتْ منْ قِبلِ باحثينَ في جامعةِ كارولينا الشماليةِ وجامعةِ ولايةِ أريزونا؛ بحيثُ تُضبطُ الركبةُ التي تعملُ بالطاقةِ لتتناسبَ معَ المريضِ. ومنَ الجديرِ بالذكرِ أنّ هذا النظامَ يعتمدُ على التعلّمِ المُعززِ، ويحاولُ باحثونَ آخرونَ تطويرَ تِقْنيّاتٍ أُخرى مبتكرةٍ، تهدفُ إلى تحسينِ حياةِ الأشخاصِ مبتوري الأطرافِ، منْ ثمَّ تمكينِهم منَ العودةِ مجددًا للقيامِ بمهامِهمْ منْ دونِ مساعدةٍ.



الشّكلُ (3-9): صورةٌ لنظامِ ساقٍ صناعيةٍ

- **العملياتُ الجراحيةُ:** يُستخدمُ الروبوتُ (Da Vinci surgical robot) في عددٍ كبيرٍ منَ العملياتِ الجراحيةِ في الولاياتِ المتحدةِ الأمريكيةِ؛ ممّا انعكسَ على العملياتِ الجراحيةِ لتصبحَ أكثرَ دقةً وأمانًا، ويساعدُ ذلكَ الجراحينَ ويعززُ قدراتِهمْ؛ حيثُ إنّ الروبوتَ يصلُ إلى أجزاءٍ منَ الجسمِ لا تستطيعُ الأيدي البشريةُ الوصولَ إليها.

3. **الخدماتُ:** تُستخدمُ الروبوتاتُ في مجالِ الخدماتِ في الفنادقِ والمستشفياتِ والجامعاتِ؛ للقيامِ بخدماتٍ مختلفةٍ، مثلَ إيصالِ الطعامِ والأدويةِ في المستشفياتِ، وخدمةِ العملاءِ وغيرِها، ومنَ الأمثلةِ على هذهِ الروبوتاتِ: روبوتٌ يعملُ على خدمةِ العملاءِ في الفندقِ. (الشّكلُ (3-10)، وروبوتُ Moxi الذي يتحملُ مسؤولياتٍ لوجستيةً في المستشفياتِ، بينما يعملُ الروبوت Co-Bot على التجوُّلِ داخلَ جامعةِ كارنيجي ميلون، ويقدمُ المساعدةَ في حالِ سُئِلَ عنْ مكتبٍ معينٍ.

الشّكلُ (3-10): روبوتاتُ الخدماتِ

4. **النقلُ**: يسهمُ استخدامُ الروبوتِ في قطاعِ النقلِ في تحسينِ الكفاءةِ، وزيادةِ الأمانِ، وتسهيلِ العملياتِ، ويعتمدُ استخدامُ الروبوتاتِ في النقلِ على مجموعةٍ منَ التِقْنيّاتِ الحديثةِ، بما في ذلكَ التعلّمُ الآليُّ، وتِقْنيّاتُ الاستشعارِ، والاتصالاتُ اللاسلكيةُ؛ ممّا يتيحُ تطويرَ حلولٍ مبتكرةٍ لمواجهةِ تحدياتِ النقلِ التقليديةِ، والاستجابةِ للمواقفِ الحرجةِ بشكلٍ سريعٍ. ومنَ الأمثلةِ عليها: السياراتُ ذاتيةُ القيادةِ.

5. **الاستكشافُ في البيئاتِ الخطيرةِ**: تُستخدمُ الروبوتاتُ لجمعِ البياناتِ والمعلوماتِ في المواقعِ الخطرةِ التي لا يمكنُ الوصولُ إليها منْ قِبلِ الإنسانِ، مثلَ استكشافِ فوهةِ بركانٍ نشطٍ، أوْ جمعِ المعلوماتِ، ورسمِ الخرائطِ لما تحتَ سطحِ الماءِ، بما في ذلكَ السفنُ الغارقةُ، أوِ استكشافُ الفضاءِ؛ ممّا يجنِّبُهُ أخطارًا كثيرةً. فمثلًا: استُخدمَ روبوتٌ متخصصٌ لرسمِ خريطةٍ لمنجمٍ فحمٍ مهجورٍ، كما يظهرُ في الشّكلِ (3-11)، واستُخدمَ أيضًا في تنظيفِ النُّفاياتِ النوويةِ، وكذلكَ في مساعدةِ طواقمِ البحثِ بعدَ انهيارِ مركزِ التجارةِ العالميِّ.

الشّكلُ (3-11): روبوتاتُ الاستكشافِ

6. **الصناعةُ**: تُستخدمُ الروبوتاتُ للقيامِ بالأعمالِ الصعبةِ، أوِ الخطرةِ أوِ الدقيقةِ أوِ المُملّةِ بالنسبةِ للبشرِ، وتُستخدمُ غالبيةُ الروبوتاتِ الصناعيةِ في مصانعِ السياراتِ، وفي عملياتِ تجميعِ القطعِ وتثبيتِها في أماكنِها، وكذلكَ في نقلِ البضائعِ والقطعِ؛ ما يزيدُ الإنتاجيةَ والكفاءةَ.

الشّكلُ (3-12): الروبوتاتُ الصناعيةُ

7. **الروبوتُ في التعليمِ**: يُستخدمُ الروبوتُ في التعليمِ؛ منْ أجلِ تعزيزِ عمليةِ التعلّمِ، وتحفيزِ الطلبةِ، وجعلِها أكثرَ متعةً، ومنَ الأمثلةِ عليهِ: روبوتُ (LEGO Minstorms) الذي يُستخدمُ لتعليمِ البرمجةِ، وكذلكَ روبوتُ EMYS الذي يُستخدمُ لتعليمِ اللغاتِ الأجنبيةِ وغيرِها منَ الروبوتاتِ

إثراء

EMYS هوَ روبوتٌ اجتماعيٌّ مصمَّمٌ لتعليمِ الأطفالِ اللغاتِ الأجنبيةَ بطريقةٍ تفاعليةٍ وممتعة، ويتميزُ بقدرتِهِ على التفاعلِ معَ الأطفالِ عنْ طريقِ تعابيرِ الوجهِ، والصوتِ، والحركةِ؛ مما يجعلهُ شريكًا تعليميًّا فريدًا، ويمكنُ استكشافُ المزيدِ منَ المعلوماتِ حولَ الروبوتِ بزيارةِ الموقعِ الإلكترونيِّ الآتي:

https://us.softbankrobotics.com/nao

نشاط جماعي

أبحثُ معَ زملائي في المواقعِ الإلكترونيةِ الموثوقةِ عنِ الروبوتاتِ التي ظهرتْ في عامِ 2024م على هيئةِ إنسانٍ آليٍّ، ثمّ أستخدمُ أحدَ برامجِ الذكاءِ الاصطناعيِّ وتطبيقاتِهِ؛ لتصميمِ فيديو يعرضُ صورةَ الروبوتِ واسمَهُ وخصائصَهُ ووظائفَهُ. بالإضافةِ إلى الدولةِ والشركةِ المصنعةِ معَ شعارِها. بعدَ ذلكَ، أستخدمُ تطبيقاتِ الذكاءِ الاصطناعيِّ التي تحوِّلُ النصَّ إلى صوتٍ لإضافةِ التعليقِ الصوتيِّ على الفيديو، ثمَّ أُشاركُ الفيديو معَ زملائي على اللوحِ التفاعليِّ الرَّقْميِّ للصفِّ، وإجراءِ نقاشٍ حولَهُ.

المُواطَنةُ الرَّقْميةُ

- **الملكيةَ الفكريةَ**: يجبُ مراعاةُ قوانينِ الملكيةِ الفكريةِ، وتوثيقُ المعلوماتِ التي أحصلُ عليها منْ مصادرِها.
- **تحمُّلَ المسؤوليةِ**: عندِ تطويرِ أوِ استخدامِ الروبوتاتِ، يجبُ أنْ يتحملَ المبرمجونَ والمستخدمونَ المسؤوليةَ عنْ أيِّ خطأٍ.
- **الاستخدامَ المسؤولَ للتكنولوجيا**: قبلَ استخدامِ الروبوتاتِ، منَ المهمِّ أنْ يتلقى المستخدمونَ تعليماتٍ واضحةً حولَ كيفيةِ استخدامِها بأمانٍ ومسؤوليةٍ.
- **التعلّمَ المستمرَّ**: الاستمرارُ في البحثِ عنْ كلِّ ما هوَ جديدٍ في مجالِ الروبوتاتِ ومشاركةِ الآخرينَ فيهِ

مشروع

المشروعُ: إنتاجُ سلسلةٍ منْ مقاطعِ الفيديو التعليميةِ (الرسومِ المتحركةِ) على شكلِ حلْقاتٍ؛ حيثُ تتناولُ كلُّ حلْقةٍ موضوعًا محددًا باستخدامِ تطبيقاتِ الذكاءِ الاصطناعيِّ/ المهمةُ 3

سأعملُ معَ زملائي على استكمالِ إعدادِ الحلْقةِ الثالثةِ ضمنَ سلسلةِ الحلْقاتِ التعليميةِ (الرسومِ المتحركةِ) وتنفيذِ الخطواتِ الآتيةِ.

- التعديلِ على الفيديوهاتِ في المهمةِ 2 بإضافةِ أمثلةٍ على روبوتاتٍ في المجالاتِ التي عُملَ عليها.
- إعدادِ لوحةٍ قصصيةٍ (Storyboards) تفصيليةٍ أساسيةٍ للحلقةِ 3 الخاصّةِ بالروبوتِ؛ بحيثُ تشملُ تحديدَ الشخصياتِ، والحوارَ المكتوبَ والمسموعَ، والخلفياتِ، والتسلسلَ البصريَّ للمشاهدِ التي تُستخدمُ كمرجعٍ أساسيٍّ في أثناءِ إنتاجِ الفيديو.
- إنتاجِ الحلْقةِ الثالثةِ التي تتحدثُ عنِ الروبوتاتِ ونشأتِها ومكوناتِها.
- إضافةِ إنجازاتٍ محليةٍ وعربيةٍ.
- مراعاةِ قواعدِ إعدادِ الحلْقاتِ التعليميةِ المذكورةِ في المهمةِ 2.

أقيّمُ تعلُّمي

المعرفةُ: أوظفُ في هذا الدرسِ ما تعلمتُهُ منْ معارفَ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأوّلُ: أُعرِّفُ المصطلحاتِ الآتيةَ: الروبوتَ، المستشعرَ.

.....

السؤالُ الثاني: أصنِّفُ الروبوتاتَ بحسبِ معيارِ قابليتِها للحركةِ.

.....

السؤالُ الثالثُ: أُقارنُ بينَ أنواعِ الروبوتِ منْ حيثُ الشّكلُ والوظيفةُ.

.....

المهاراتُ: أوظفُ مهاراتِ التفكيرِ الناقدِ، والتواصلَ الرَّقْميَّ، والبحثَ الرَّقْميَّ في الإجابةِ عنِ السؤاليْنِ الآتييْنِ:

السؤالُ الأوّلُ: أبحثُ عنِ اسمِ روبوتٍ مستخدمٍ في كلِّ قطاعٍ ممّا يأتي، والشركةِ المصنعةِ لهُ، وأذكرُ أهميةَ استخدامِهِ:

القطاعُ	اسمُ الروبوتِ	الشركةُ المصنعةُ لهُ	أهميةُ استخدامِهِ
التعليمُ			
القطاعُ الأمنيُّ			
قطاعُ السياحةِ			

السؤالُ الثاني: ما المجالُ الذي أرغبُ بتصميمِ روبوتٍ منْ أجلِهِ؟ وما هيَ استخداماتُهُ والقيمةُ التي سيضيفُها هذا الروبوتُ في هذا المجالِ؟

.....

السؤالُ الثالثُ: أرسمُ الهيكلَ المناسبَ لهذا الروبوتِ، مراعيًا أنْ يخدمَ الهيكلُ الهدفَ الذي سيُصمَّمُ الروبوتُ لأجلِهِ؛ باستخدامِ أحدِ برامجِ الرسمِ على الحاسوبِ، ثمَّ أختارُ اسمًا إبداعيًّا لهُ.

القِيمُ والاتجاهاتُ:

أستخدمُ أحدَ برامجِ الذكاءِ الاصطناعيِّ لتصميمِ بوسترٍ يضمُّ أهمَّ مواقعِ الذكاءِ الاصطناعيِّ التعليميةِ المفيدةِ للطلبةِ ومواقعِها الإلكترونيةِ، مرفقًا رموزًا سريعةَ الاستجابةِ، وأنشرُهُ في المدرسةِ؛ ليكونَ معينًا للطلبةِ في تعلُّمِهمْ.

الدرسُ الرابعُ

أساسياتُ برمجةِ الروبوتِ في بيئةٍ افتراضيةٍ (Basics of Programming the Robot in a Virtual Environment)

الفكرةُ الرئيسةُ

التعرفُ إلى أساسياتِ برمجةِ الروبوتاتِ، وتطبيقُ هذهِ الأساسياتِ ببرمجةِ روبوتٍ على الحركاتِ الأساسيةِ في بيئةٍ افتراضيةٍ.

المصطلحاتُ والمفاهيمُ الرئيسةُ

محاكي الروبوتاتِ الافتراضيُّ (Virtual Robotics Simulator)، بيئاتُ العملِ (Playground)، لبناتُ الحركةِ (Movement Blocks)، لبناتُ العرضِ (Display Blocks)، لبناتُ الاستشعارِ (Sensing Blocks)، لبنةُ الجذبِ (Magnet Block).

نتاجاتُ التعلّمِ (Learning Outcomes)

أُبرمجُ الروبوتَ على الحركاتِ الأساسيةِ في بيئةٍ افتراضيةٍ.

تعرَّفنا مكوناتِ الروبوتِ الأساسيةَ، وتعلَّمْنا أيضًا أنْ الروبوتَ يجبُ برمجتُهُ لأداءِ مهامَّ محددةٍ بطريقةٍ مستقلةٍ أوْ شبهِ مستقلةٍ؛ بكتابةِ التعليماتِ البرمجيةِ، منْ أوامرَ وخوارزمياتٍ، تُمكِّنُ الروبوتَ منَ التفاعلِ معَ بيئتِهِ واتخاذِ قراراتٍ بناءً على المدخلاتِ التي يتلقاها منَ المستشعراتِ. فما أساسياتُ برمجةِ الروبوتِ؟ وكيفَ نكتبُ هذهِ التعليماتِ ونفحصُها؟

منتجاتُ التعلّمِ

إعدادُ مقاطعِ فيديو لبرامجِ محاكاةٍ خاصةٍ بالروبوتاتِ في بيئاتٍ افتراضيةٍ.

إعدادُ عرضٍ تقديميٍّ باستخدامِ (Google Slides)، يوّضحُ خطواتِ عملِ إنجازِ المهامِّ داخلَ بيئةِ محاكاةِ الروبوتِ.

نشاط تمهيدي

- أفتحُ برنامجَ سكراتش على جهازي، (ويمكنُني استخدامُ نسخةِ الويبِ عنْ طريقِ زيارةِ موقعِ سكراتش الرسميِّ).
- يمكنُ رسمُ متاهةٍ يدويًّا داخلَ سكراتش باستخدامِ أدواتِ الرسمِ، أوْ تحميلِ صورةٍ جاهزةٍ لمتاهةٍ تحتوي بوابتينِ.
- أختارُ كائنًا منْ مكتبةِ سكراتش، أوْ أرسمُ كائنًا جديدًا، بحيثُ يكونُ هذا الكائنُ اللاعبَ الذي سيحاولُ الخروجَ منَ المتاهةِ.
- أستخدمُ الأوامرَ البرمجيةَ في سكراتش؛ لجعلِ الكائنِ يتحركُ داخلَ المتاهةِ، ويمكنُني استخدامُ الأسهمِ للتحكمِ فيهِ، أوْ برمجتِهِ ليتحركَ تلقائيًّا
- أُضيفُ لبناتِ برمجةٍ للكشفِ عنِ التصادمِ معَ الجدرانِ أوِ العوائقِ لتجنُّبها. مثلًا، أستخدمُ لبنةَ "إذا على حافة، ارتد" أوْ اصنعْ شرطًا يتحققُ منَ التصادمِ معَ لونٍ معينٍ يمثلُ الجدرانَ.
- أُشغّلُ البرنامجَ لمعرفةِ ما إذا كانَ الكائنُ يتمكنُ منَ الوصولِ إلى البوابةِ بنجاحٍ منْ دونِ الاصطدامِ بالعوائقِ، وأعدِّلُ الكودَ بحسبِ الحاجةِ لضمانِ عملِهِ كما يجبُ.
- أُشاركُ مشروعي معَ زملائي أوْ على موقعِ سكراتش ليراهُ الآخرونَ.

أساسياتُ برمجةِ الروبوتاتِ

تختلفُ مكوناتُ الروبوتِ والمستشعراتِ المستخدمةِ فيهِ باختلافِ المهمةِ التي يؤديها لذا؛ فإنَّ برمجتَهُ كذلكَ تختلفُ، فمثلًا، برمجةُ روبوتٍ صناعيٍّ تتطلبُ تعليماتٍ دقيقةً لتنفيذِ مهامَّ متكررةٍ بدقةٍ عاليةٍ في بيئةٍ محددةٍ مثلَ خطوطِ الإنتاجِ، بينما برمجةُ روبوتٍ متحركٍ (مثلَ روبوتِ تنظيفِ المنازلِ) تتطلبُ خوارزمياتٍ للتنقلِ، وتجنُّبِ العقباتِ والعملِ في بيئةٍ ديناميكيةٍ. بالإضافةِ إلى ذلكَ، تختلفُ لغاتُ البرمجةِ، وأدواتُ التطويرِ؛ بناءً على متطلباتِ الأداءِ والتفاعلِ في كلِّ نوعٍ منَ الروبوتاتِ.

تعدُّ خطـــوةُ تحديدِ المكوناتِ الأساســـيةِ للروبوتِ، منْ متحكمٍ ومستشـــعراتٍ وقِطَعٍ كهربائيةٍ وميكانيكيةٍ، وتحديدِ المهامِّ المتوقعِ منَ الروبوتِ إنجازُها، والبيئةِ التي ستُنفَّذُ هذهِ المهامُّ داخلَها مهمةً أساسيةً تســـبقُ البدءَ بعمليةِ البرمجةِ. منَ الواضحِ أنَّ هذهِ المكوناتِ، قدْ لا تكونُ بصورتِها النهائيةِ؛ لأنَّ كلَّ جزءٍ من الأجزاءِ المذكورةِ قدْ يُســـتبدلُ لعدمِ انسجامِهِ معَ المهامِّ المطلوبةِ. فعلى ســـبيلِ المثالِ، قدْ يُستخدمُ محركٌ آخرُ للعجلاتِ بعزمٍ أكبرَ للقدرةِ على إنجازِ المهامِّ المقترحةِ في بيئةِ العملِ، أوْ قدْ نلجأُ لتعديلِ عددٍ أوْ/ ونوعِ المستشعراتِ للسببِ نفسِهِ.

وكما تعلَّمْنا مســـبقًا، فإنَّ عمليةَ البرمجةِ هيَ عمليةٌ دوريةٌ تُكتـــبُ خلالَها التعليماتُ وتُختبرُ، منْ ثمَّ تُعـــدَّلُ إذا لزمَ؛ حتى نصلَ إلى آليةِ عملٍ ومخرجاتٍ تطابـــقُ المطلوبَ. وفي ما يتعلقُ ببرمجةِ الروبوتـــاتِ، فإنَّ مكوناتِ النظامِ متنوعةٌ، وقد يأتي الخَلَلُ منْ أكثرَ منْ مصدرٍ، وإنَّ وجودَ أيِّ خَللٍ قدْ يُسببُ بعدمِ اســـتجابةِ الروبوتِ، أوْ بوقوعِهِ أوْ اصطدامِهِ بحواجزَ وغيرِها منَ الحالاتِ التي قدْ تكونُ مكلفةً، خاصّةً في المراحلِ الأولى لبرمجةِ الروبوتِ وفحصِهِ. لذلكَ يُفضّلُ فحصُ الروبوتِ في بيئاتٍ افتراضيةٍ (Virtual Robotics Simulator) تحاكي الواقعَ.

استعمالُ البيئةِ الافتراضيةِ للتطويرِ لهُ ميزاتٌ عِدّةٌ، منها:

- السلامةُ.
- سهولةُ الوصولِ والتجريبِ.
- القدرةُ على التَّكرارِ السريعِ للتجاربِ.
- تقليلُ الكلفةِ.
- سهولةُ تطويرِ بيئاتِ عملٍ بظروفٍ وتحدياتٍ مختلفةٍ.

على الرغمِ منْ فعاليةِ البيئةِ الافتراضيةِ، فإنَّ عملَ الروبوتِ في البيئةِ الافتراضيةِ، قدْ لا يعني بالضرورةِ أنَّ الروبوتَ سيعملُ بشكلٍ جيّدٍ في البيئةِ الحقيقيةِ؛ لأنَّ هناكَ ظروفًا ومتغيراتٍ أُخرى قدْ لا تكونُ أُخذتْ بعينِ الاعتبارِ خـــلالَ عمليةِ التطويرِ في البيئةِ الافتراضيةِ، مثلَ وزنِ الروبوتِ، والاحتكاكِ، ومستوى الإضاءةِ، والضوضاءِ، وعواملَ أُخرى.

مُحاكي الروبوتاتِ الافتراضيُّ (Virtual Robotics Simulator)

مُحاكي الروبوتاتِ الافتراضيُّ: هوَ أداةٌ تُستخدمُ لتصميمِ الروبوتاتِ وتطويرِها واختبارِها في بيئةٍ محاكيةٍ للواقعِ منْ دونِ الحاجةِ إلى المكوناتِ الفيزيائيةِ. محاكي (VEX) الافتراضيُّ، يُعدُّ منَ المحاكياتِ الفعّالةِ التي يمكنُ الاعتمادُ عليها لبرمجةِ الروبوتاتِ منْ نوعِ (VEX)؛ حيثُ يوفّرُ هذا المحاكيَ البرمجةَ باستخدامِ لغةِ البرمجةِ (Python)، أوْ باستخدامِ اللبناتِ الجاهزةِ التي تُحوَّلُ ضمنيًّا وتلقائيًّا إلى برامجَ، ويُشبهُ المحاكي (VEX) بدرجةٍ كبيرةٍ واجهةَ برنامجِ (Scratch) معَ اختلافاتٍ بسيطةٍ تتوافقُ معَ الروبوتاتِ وآليةِ عملِها.

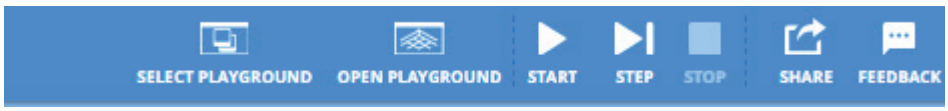
نشاط عملي

أستكشفُ موقعَ محاكي الروبوتِ الافتراضيِّ (VEX)، وأُقارنُ بينَ اللبناتِ البرمجيةِ المتاحةِ في (VEX) واللبناتِ الموجودةِ في برمجيةِ سكراتش . بعدَ إتمامِ المقارنةِ، أُشاركُ ما توصلتُ إليهِ معَ زملائي في الصفِّ بالنقاشِ، وأتبادلُ الأفكارَ حولَ الفروقاتِ والتشابهاتِ بينَ النظاميْنِ.

https://vr.vex.com/

بيئةُ العملِ (Playground)

يركزُ مُحاكي (VEX)على التحكّمِ بسيارةٍ تتحركُ في بيئةِ عملٍ افتراضيةٍ والقيامِ بمهامَّ معينةٍ، وتتنوعُ بيئاتُ العملِ الموجودةُ بينَ بيئةٍ خاليةٍ منَ العناصرِ، منْ حواجزَ وخطوطٍ، إلى بيئةٍ يتوافرُ فيها حواجزُ وخطوطٌ وأقراصُ وبناياتٌ ومتاهاتٌ. ويمكنُنا التعرّفُ إلى هذهِ البيئاتِ بالضغطِ على زرِّ اختيارِ بيئةِ العملِ (Select Playground).



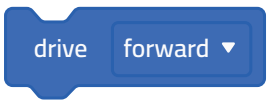
تتكونُ بيئةُ العملِ منْ لبناتٍ مختلفةٍ، سنتعرفُ إليها في ما يأتي:

لبناتُ الحركةِ (Movement Blocks):

تساعدُ لبناتُ الحركةِ على التحكّمِ بحركةِ الروبوتِ منْ جهةِ السرعةِ والاتجاهِ والزاويةِ.

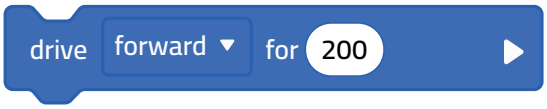
- **السرعةُ**: تكونُ السرعةُ نسبةً للسرعةِ الحاليةِ.

- **الاتجاهُ**: يدعمُ الحركةَ للأمامِ أوْ للخلفِ.



- **الزاويةُ**: تُحدّدُ زاويةُ الدورانِ

- **المسافةُ**: تُحدّدُ المسافةُ التي يقطعُها الروبوتُ.



نشاط فردي

أقومُ بتشغيلِ البرنامجِ، وأُؤدي المهامَّ الآتيةَ منفصلةً.

1 – أعملُ مشروعًا جديدًا بالذهابِ إلى قائمةِ (File)، واختيارِ (New Blocks Project).

2 – أختارُ بيئةَ العملِ (Grid Map).

3 – **أضعُ اللبناتِ البرمجيةَ المناسبةَ لإنجازِ ما يأتي:**

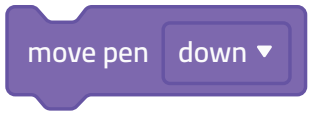
- تحريكِ الروبوتِ للأمامِ بسرعةٍ ثابتةٍ حتى يصطدمَ بالجدارِ.
- التفافِ الروبوتِ 90 درجةً لليمينِ، ثمَّ يتحركُ للأمامِ بسرعةٍ ثابتةٍ حتى يصطدمَ بالجدارِ.
- تحريكِ الروبوتِ للأمامِ بسرعةٍ ثابتةٍ لمسافةِ 800mm ثمَّ يتوقفُ.
- تحريكِ الروبوتِ للأمامِ بسرعةٍ ثابتةٍ لمسافةِ 800mm ، ثمّ يعودُ للخلفِ 400mm منْ دونْ الالتفافِ

لِبناتُ العرضِ (Display Blocks):

باستخدامِ لبناتِ العرضِ، نستطيعُ التحكّمُ بالروبوتِ لرسمِ خطٍّ بحسبِ المسارِ المخصصِ لهُ، معَ إمكانيةِ تحديدِ لونِ الخطِّ

عن طريق اللبنات الآتية:

- **لبنةِ تفعيلِ الرسمِ**: عنْ طريقِ هذهِ اللبنةِ، نقومُ بالكتابةِ عندَما تكونُ القيمةُ (down)، ووقفِ الكتابةِ عندَما تكونُ القيمةُ (up).



- **لبنةِ لونِ الخطِّ**: تساعدُ هذهِ اللَّبنةُ على تحديدِ لونِ الخطِّ المرسومِ.

نشاط جماعي

أتعاونُ معَ زملائي لاستخدامِ لبناتِ الحركةِ، ولبناتِ العرضِ لبرمجةِ الروبوتِ؛ حتى يسيرَ بمسارٍ مربعٍ، طولُ ضلعِه 400 مم داخلَ بيئةِ Art Canvas، وفي أثناءِ حركتِهِ، سيرسمُ الروبوتُ شكلَ مربعٍ. بعدَ إتمامِ البرمجةِ، سنناقشُ النتائجَ ونعرضُها على بقيةِ الزملاءِ في الصفِّ.

لبناتُ الاستشعارِ (Sensing Blocks):

لتتمكَّنَ منَ التحكمِ بالروبوتِ، تساعدُ المُستشعِراتُ على إدراكِ العناصرِ المحيطةِ بالروبوتِ منْ جهةِ وجودِها منْ عدمِهِ، أو خصائصِهِ مثلَ اللونِ.

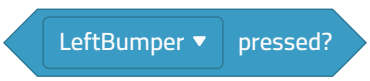
توجدُ أنواعٌ عدةٌ منَ المُستشعِراتِ في (VEX) نذكرُ منها:

- **مُستشعِرَ المسافةِ:** يُستعملُ هذا المستشعرُ في تحديدِ بُعدِ العنصرِ عنْ مقدمةِ السيارةِ.

- **مستشعرَ اللونِ:** يُستعملُ لتحديدِ لونِ العنصرِ الموجودِ أمامَ السيارةِ أوْ أسفلَها

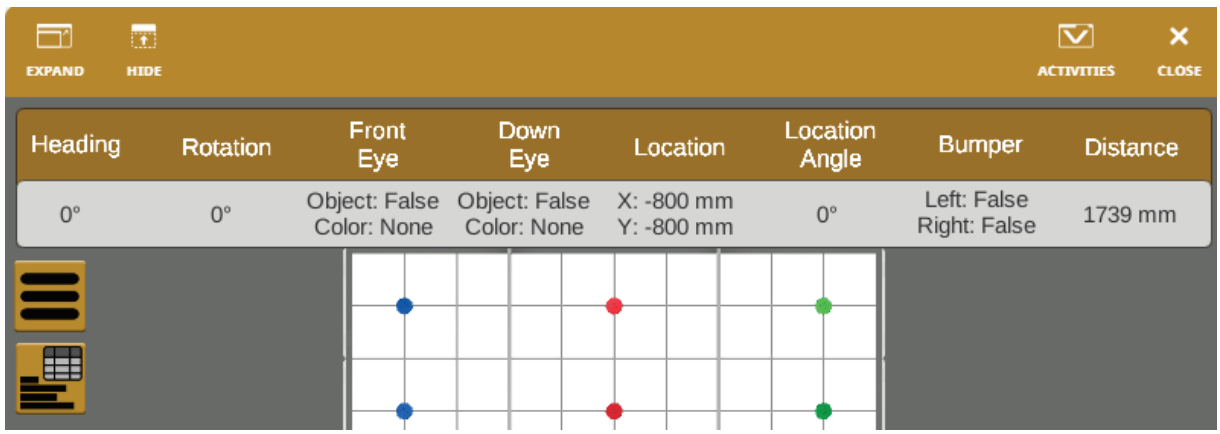
- **مستشعرَ الموقعِ:** يُستعملُ لمعرفةِ إحداثياتِ الروبوتِ الأفقيةِ والعموديةِ.

- **مستشعرَ الحركةِ:** يُستعملُ لمعرفةِ زاويةِ مسيرِ السيارةِ أوْ زاويةِ دورانِها



- **مستشعرَ التصادمِ:** يُستعملُ لمعرفةِ ما إذا كانَ هناكَ تصادمٌ بينَ واجهةِ الروبوتِ الأماميةِ منْ جهةِ اليمينِ أوْ جهةِ اليسارِ.

يمكنُ معرفةُ قِيَمِ هذهِ المستشعراتِ خلالَ حركةِ الروبوتِ عندَ الضغطِ علىَ زرِّ لوحةِ القيادةِ (Dashboard)

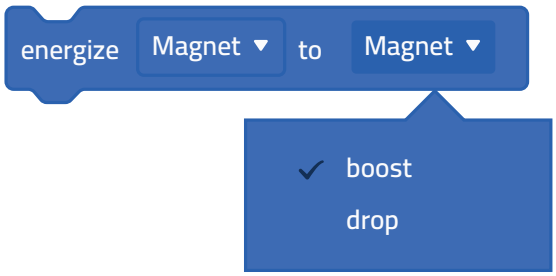


نشاط فردي

بناءً على ما تعلمتُهُ مسبقًا في لغاتِ البرمجةِ والخوارزمياتِ، ما الفرقُ بينَ اللبناتِ البيضاويةِ السداسيةِ في البرمجةِ؟ كما هوَ مُوضّحٌ في الصورِ الآتيةِ:

أناقشُ زملائي معَ ذكرِ أمثلةٍ أُخرى.

لبِنةُ الجذبِ (Magnet Block):



تُستخدمُ هذهِ اللّبنةُ للتعاملِ معَ الأقراصِ المعدِنيةِ القابلةِ للجذبِ، التي قدْ توجدُ في بيئةِ العملِ، وعنْ طريقِ هذهِ اللبنةِ، يمكنُ تفعيلُ خاصيةِ الجذبِ باختيارِ خيارِ (boost)، أوْ إيقافِ خاصيةِ الجذبِ عنْ طريقِ اختيارِ خيارِ (drop).

نشاط فردي

منْ قائمةِ الأمثلةِ الموجودةِ في الموقعِ، أذهبُ إلى قائمةِ (File)، أختارُ (Open Examples)، ثمَّ أختارُ مثالَ (Coral Reef Cleanup Level 1) المعنيَّ بتوظيفِ الروبوتِ لتنظيفِ الشُّعَبِ المَرجانيةِ منَ المهملاتِ، وأُحلِّلُ اللبناتِ البرمجيةَ المستخدمةَ فيهِ لتوظيفِ الروبوتِ في تنظيفِ الشعبِ المَرجانيةِ منَ المهملاتِ، وأربطُ كلَّ لبنةٍ بما يقومُ بهِ الروبوتُ فعليًّا في الأداءِ.

أُعدِّلُ أداءَ الروبوتِ؛ بحيثُ يتمكنُ منْ إزالةِ مجسميْنِ منَ المهملاتِ، وأُقارنُ حلّي معَ المثالِ (Coral Reef Cleanup Level 2) الذي يوظفُ مُستشعرَ المسافةِ لتحديدِ موقعِ المهملاتِ.

أُعدِّلُ على الأمثلةِ؛ حتى يتمكنَ الروبوتُ منْ جمعِ عددٍ أكبرَ منَ المجسماتِ، ثمَّ أُناقشُ النتائجَ والتعديلاتِ معَ زملائي في الصفِّ

نشاط عملي

عملُ مجموعاتٍ

أتعاونُ معَ زملائي في المجموعةِ لاستخدامِ لبناتِ الحركةِ والاستشعارِ والجذبِ لبرمجةِ الروبوتِ في بيئةِ (Disk Mover)؛ لإحضارِ أوّلِ قرصٍ أزرقَ موجودٍ، ووضعِهِ داخلَ المربعِ الأزرقِ، معَ العلمِ أنَّ إحداثياتِ القرصِ العموديِّ والأفقيِّ معروفةٌ مسبقًا؛ حيثُ إنَّ كلَّ مربعٍ في بيئةِ العملِ أبعادُهُ 200mm X 200mm.

سأبدأُ بتجزئةِ المشكلةِ إلى مشكلاتٍ أصغرَ لتسهيلِ الحلِّ، وذلكَ عبرَ الخطواتِ الآتيةِ:

- أذهبُ إلى الأمثلةِ المتاحةِ، وأختارُ مثالَ (Moving Disks)، وأشغِّلُهُ، ثمَّ أُناقشُ معَ أفرادِ المجموعةِ آليةَ العملِ، وكيفيةَ حركةِ الروبوتِ.
- أُعدِّلُ المثالَ ليتمكنَ الروبوتُ منْ إحضارِ القرصِ الأزرقِ الأوّلِ، والثاني، والثالثِ بالطريقةِ نفسِها، ووضعِهم داخلَ المربعِ الأزرقِ.
- أعدّلُ المثالَ الأوّلَ؛ بحيثُ يَستخدمُ الروبوتُ لبنةَ مستشعرِ الألوانِ لإحضارِ القرصِ الأزرقِ الأوّلِ، ووضعِهِ في المربعِ الأزرقِ.
- أُعدّلُ البرنامجَ بإحضارِ الأقراصِ الثلاثةِ ذاتِ اللونِ الأزرقِ، ووضعِها في المربعِ الأزرقِ باستخدامِ لبناتِ الحركةِ والاستشعارِ والجذبِ.

نشاركُ نتائجَنا معَ الزملاءِ، ونناقشُ التحدياتِ، ونتبادلُ الملاحظاتِ.

المُواطَنةُ الرَّقْميةُ

- **الاستثمارَ الإيجابيَّ**: أُوظفُ ما تعلمتُهُ لتطويرِ مهاراتي، ومواكبةِ التطوراتِ، واستشرافِ المستقبلِ.
- **التعاونَ الرَّقْميَّ**: أعزِّزُ قيمَ التضامنِ والتعاونِ والمعاملةِ بإيجابيةٍ معَ الزملاءِ في أثناءِ العملِ على المهامِّ والمشروعاتِ.
- **الخصوصيةَ الرَّقْميةَ**: أحرصُ على حمايةِ عملي وعملِ المجموعاتِ، وأُحافظُ على خصوصيةِ الآخرينَ.
- **المسؤوليةَ والنُّظمَ**: أكونُ مسؤولًا عن تعاملي معَ العالمِ الرَّقْميِّ، وأحترمُ القوانينَ والقواعدَ المنظمةَ لذلكَ

مشروع

المشروعُ: إنتاجُ سلسلةٍ منْ مقاطعِ الفيديو التعليميةِ (الرسومِ المتحركةِ) على شكلِ حلْقاتٍ؛ بحيثُ تتناولُ كلُّ حلْقةٍ موضوعًا محددًا باستخدامِ تطبيقاتِ الذكاءِ الاصطناعيِّ/ المهمةُ 4

سأستكملُ معَ زملائي سلسلةَ الحلْقاتِ التعليميةِ (الرسومِ المتحركةِ)، ونقومُ بإعدادِ الحلْقةِ التعليميةِ السابعةِ بتنفيذِ الخطواتِ الآتيةِ:

- **استخدامِ بيئةِ مُحاكاةِ الروبوتِ**: نُنجزُ مهامَّ محددةً داخلَ بيئةِ محاكاةِ الروبوتِ، معَ تسجيلِ الشاشةِ في أثناءِ العملِ لإظهارِ كيفيةِ تنفيذِ المهامّ، ثمَّ نضيفُ صوتًا يشرحُ الخطواتِ والمهامَّ التي تُنفَّذُ خلالَ عمليةِ التسجيلِ.
- **إنتاجِ الفيديو**: نُنتجُ فيديو يعرضُ الخطواتِ العمليةَ التي اتَّبعْناها في البيئةِ الافتراضيةِ، معَ التركيزِ على الوضوحِ والدقةِ في شرحِ المهامِّ.
- **المراجعةِ والتحسينِ**: نراجعُ الحلْقاتِ السابقةَ في السلسلةِ، ونجري التحسيناتِ اللازمةَ لضمانِ جودةِ العرضِ التعليميِّ.
- **التقييمِ الذاتيِّ**: أُقيِّمُ الفيديو والحلقةَ بناءً على المعاييرِ التي حدّدها المعلمُ في المهامِّ السابقةِ، معَ إجراءِ التعديلاتِ المطلوبةِ؛ لتحسينِ العملِ وفقًا للملاحظاتِ.
- **مشاركةِ النتائجِ**: نُشاركُ النتائجَ معَ المجموعاتِ الأخرى، ونستفيدُ منْ ملاحظاتِهم لتحسينِ جودةِ الحلْقاتِ التعليميةِ، وبعدَ مراجعةِ الحلْقاتِ، نُطلقُ اسمًا مناسبًا على السلسلةِ التعليميةِ؛ لنشرِها وجعلِها متاحةً للجمهورِ التعليميِّ عبرَ المنصةِ التعليميةِ التي تستخدمُها المدرسةُ عنْ طريقِ المعلمِ، أوْ عبرَ قناةٍ مخصّصةٍ للفيديوهاتِ.

أقيّمُ تعلمي

المعرفةُ: أُوظّفُ في هذا الدرسِ ما تعلمتُهُ منْ معارفَ في الإجابةِ عنِ السؤالينِ الآتيين:

السؤالُ الأوّلُ: أُبينُ دورَ برمجةِ الروبوتِ في القيامِ بمهامِهِ المتوقعةِ.

.....

.....

.....

السؤالُ الثاني: أُبينُ أنواعَ اللبناتِ المتوافرةِ في بيئةِ المحاكاةِ الافتراضيةِ (VEX).

.....

.....

.....

المهاراتُ: أُوظفُ مهاراتِ التفكيرِ الناقدِ والتواصلِ الرَّقْميِّ والبحثِ الرَّقْميِّ في الإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأوّلُ: أُبينُ سلبياتِ استخدامِ المُحاكي الافتراضيِّ لبرمجةِ الروبوتِ.

.....

.....

.....

السؤالُ الثاني: أبحثُ في أنواعِ المستشعراتِ التي يمكنُ إضافتُها للروبوتِ (VEX) والمهامِّ الجديدةِ التي قدْ نحصلُ عليها منْ إضافتِها.

.....

.....

.....

السؤالُ الثالثُ: أُبينُ المهمةَ التي يقومُ بها هذا الروبوتُ إذا تمتْ برمجتُهُ كما يظهرُ في الشّكلِ الآتي:

السؤالُ الرابعُ: أبحثُ في ميزاتِ المحاكي الافتراضيِّ VEX، وأستخدمُها في برمجةِ الروبوتِ على حركاتٍ جديدةٍ.

.....

.....

.....

القِيمُ والاتجاهاتُ

أُطلقُ مبادرةً في مدرستي لتعليمِ أساســـياتِ برمجةِ الروبوتِ للطلبةِ في صفّيِ السابعِ والثامنِ، ثمَّ أُنظِّمُ معَ مُعلمِيِّ الأوقاتَ، وأعدادَ الطلبةِ، وآليةَ التنفيذِ.

ملخصُ الوَحْدةِ

تعلمتُ في هذهِ الوَحْدةِ مفهومَ الذكاءِ الاصطناعيِّ وخصائصِهُ وميزاتِهِ وتطبيقاتِهِ، ومفهومَ الروبوتِ وبرمجتَهُ في بيئةِ المُحاكي الافتراضيِّ، وفي ما يأتي أبرزُ الجوانبِ التي تناولَتْها الوَحْدةُ:

- **الذكاءُ الاصطناعيُّ**: هوَ عمليةُ محاكاةٍ لقدراتِ الإنسانِ، أوْ محاكاةٍ لسلوكِهِ، مثلَ التعرّفِ إلى الأشياءِ والفهمِ، والاستجابةِ للغاتِ، والقدرةِ على حلِّ المشكلاتِ واتخاذِ القرارِ.
- تُشكلُ كلٌّ منَ البياناتِ والخوارزمياتِ الخاصّةِ، والنماذجِ والتفاعلِ معَ البيئةِ المحيطةِ نظامَ الذكاءِ الاصطناعيِّ..

  ومنَ الأمثلةِ على أنظمةِ الذكاءِ الاصطناعيِّ:
  - معالجةُ اللغاتِ الطبيعيةِ،
  - وأنظمةُ التعلّمِ الآليِّ،
  - وأنظمةُ الرؤيةِ الحاسوبيةِ،
  - وأنظمةُ ذكاءٍ اصطناعيٍّ خاصةٍ بالتعليمِ،
  - وأنظمةُ التسويقِ.
- **يتميزُ الذكاءُ الاصطناعيُّ بخصائصَ عــدّةٍ، منها**: معالجةُ اللغاتِ الطبيعيــةِ، وأتمتةُ المهامِّ، واستيعابُ البياناتِ، ومحاكاةُ الإدراكِ البشريِّ، والحوســبةُ الكموميةُ، والحوسبةُ السحابيةُ، والتخطيطُ. ويتميزُ النظامُ الذكيُّ أيضًا بقدرتِهِ على التعلّمِ والإدراكِ، واستخدامِ المنطقِ، واتخاذِ القرارِ، وحلِّ المشكلاتِ، واستخدامِ اللغةِ.
- منَ المجالاتِ الحيويةِ التــي يؤثّرُ بها الذكاءُ الاصطناعيُّ التعليمُ، والرعايةُ الصحيةُ، والأعمالُ التجاريةُ، والصناعةُ، والأمنُ السيبرانيُّ، والنقلُ، والزراعةُ.
- منَ التأثيــراتِ الاجتماعيةِ الإيجابيةِ للذكاءِ الاصطناعيِّ الحفاظُ على حياةِ الإنســانِ، وتقليلُ تعرضِهِ للمخاطرِ، والتخفيفُ منْ حوادثِ الســيرِ والازدحاماتِ المروريةِ، وخلقُ فرصِ عملٍ جديدةٍ.
- منَ التأثيراتِ الســلبيةِ للذكاءِ الاصطناعيِّ، قلةُ فرصِ العملِ بسببِ إيجادِ حلولٍ فعّالةٍ لبعضِ الأعمالِ، والتأثيرُ الســلبيُّ في المهاراتِ الأساسيةِ، والتخوُّفُ منِ اختراقِ البياناتِ ومعلوماتِ

الأفرادِ؛ ممّا يؤدي إلى انتهاكِ الخصوصيةِ على مستوى الأفرادِ والمؤسساتِ.

- **الروبوتُ آلةٌ إلكترو-ميكانيكيةٌ تُبرمجُ بوساطةِ برامجَ حاسوبيةٍ خاصةٍ؛ للقيامِ بالعديدِ منَ الأعمالِ الخطرةِ والشاقّةِ والدقيقةِ، والمُملّةِ أحيانًا، ويتكونُ منَ الحسّاساتِ، والمتحكم، والمحركاتِ، والمستجيبِ النهائيِّ، وتُضافُ المفاصلُ والمشغلُ للروبوتاتِ التي تتحرَّكُ بعضُ أجزائها، وتعملُ الروبوتاتُ عنْ طريقِ ثلاثةِ مستوياتٍ هرميةٍ، هيَ:** التخطيطُ للمهمةِ، والتخطيطُ للحركةِ، وأخيرًا التحكمُ.
- تُصنَّفُ الروبوتاتُ بحسبِ شكلِها إلى روبوتاتٍ مجسمةٍ تأخذُ شكلَ مجسمٍ، وروبوتاتٍ على هيئةِ ذراعٍ، وروبوتاتٍ ذاتِ أجنحةٍ، وروبوتٍ سبّاحٍ. وقدْ يأتي الروبوتُ على شكلِ غرفةٍ كاملةٍ.
- برمجةُ الروبوتِ عمليةٌ دوريةٌ، تُكتبُ خلالَها التعليماتُ وتُختَبرُ، منْ ثمَّ يُعدَّلُ عليها إذا لزمَ الأمرُ؛ حتى نصلَ إلى آليةِ عملٍ ومخرجاتٍ تُطابقُ المطلوبَ، وتختلفُ برمجةُ الروبوتِ باختلافِ المهمةِ التي سيؤديها.
- **علمُ الروبوتاتِ:** علمٌ يقومُ على تصميمِ هذهِ الآلاتِ وبنائِها وبرمجتِها؛ لتتفاعلَ معَ البيئةِ المحيطةِ، وتجمعُ عديدًا منَ المفاهيمِ الخاصةِ بعلمِ الذكاءِ الاصطناعيِّ، منها: الإدراكُ، والتخطيطُ، والتعلّمُ غيرُ الخاضعِ للإشرافِ، والتعلُّم المعزّز.
- يُستخدمُ محاكي الروبوتِ الافتراضيُّ (VR VEX) لمحاكاةِ عملِ الروبوتِ في البيئةِ الحقيقيةِ.
- **لاستعمالِ البيئةِ الافتراضيةِ بدلًا منَ الحقيقةِ في مجالِ فحصِ الروبوتاتِ عديدٌ منَ المميزاتِ، منها:** السلامةُ، وسهولةُ الوصولِ، والتجريبُ، وتعزيزُ التعاونِ، وتبادلُ المعرفةِ بينَ أعضاءِ الفريقِ، والقدرةُ على التكرارِ السريعِ للتجاربِ، وتقليلُ الكلفةِ، وسهولةُ تطويرِ بيئاتِ العملِ بظروفٍ وتحدياتٍ مختلفةٍ

أسئلةُ الوَحْدةِ

السؤالُ الأوّلُ: أُعرِّفُ المقصودَ بكلٍّ منَ المصطلحاتِ الآتيةِ:

أنظمةُ الذكاءِ الاصطناعيِّ: .....

.....

الروبوتُ: .....

.....

الحسّاساتُ: .....

.....

السؤالُ الثاني: باستخدامِ محاكي الروبوتِ الافتراضيِّ، أُبرمجُ الروبوتَ؛ ليقومَ بتنظيفِ البيئةِ الافتراضيةِ منَ المخلفاتِ.

السؤالُ الثالثُ: أُحدِّدُ المكوّنَ الخاصَّ بالروبوتِ في كلٍّ ممّا يأتي:

أ. يُعطي الأوامرَ للروبوتَ بناءً على البياناتِ المدخلةِ منَ الحسّاساتِ .....

ب. الجزءُ النهائيُّ منَ الروبوتِ الذي يؤدي المهمةَ المطلوبةَ منهُ .....

ج. عنصرٌ أساسيٌّ للروبوتِ يحتوي على أجزاءَ متحركةٍ .....

د. يُستخدمُ لتحريكِ المفاصلِ التي تربطُ بينَ الأجسامِ الصُّلبةِ .....

هـ. تجمعُ البياناتِ منَ البيئةِ المحيطةِ .....

السؤالُ الرابعُ: ما أهميةُ استخدامِ الذكاءِ الاصطناعيِّ في كلِّ مجالٍ منَ المجالاتِ الآتيةِ؟

أ. التعليمِ:

.....

ب. السياحةِ:

.....

ج. الصناعة:

.....

السؤالُ الخامسُ: أختارُ رمزَ الإجابةِ الصحيحةِ في كلٍّ ممّا يأتي:

1. أحدُ الخياراتِ الآتيةِ يُستخدمُ في معالجةِ اللغاتِ الطبيعيةِ في الذكاءِ الاصطناعيِّ:

أ. الحوسبةُ السحابيةُ.

ب. تحويلُ الكلامِ المنطوقِ إلى نصٍّ.

ج. الحوسبةُ الكموميةُ.

د. تحديدُ الأهدافِ، والعملُ على بلوغِها.

2. الفائدةُ الرئيسةُ لأتمتةِ المهامِّ البسيطةِ والمتكررةِ باستخدامِ الذكاءِ الاصطناعيِّ:

أ. زيادةُ كميةِ البياناتِ التي تُجْمَعُ.

ب. تحويلُ الأنشطةِ اليدويةِ إلى أنشطةٍ حاسوبيةٍ.

ج. تحسينُ استجابةِ برامجِ الدردشةِ الآليةِ.

د. استخدامُ الحوسبةِ السحابيةِ.

3. إحدى المهامِّ الآتيةِ تعدُّ منْ مميزاتِ الذكاءِ الاصطناعيِّ في مجالِ التخطيطِ:

أ. تحديدُ الأهدافِ والعملُ على بلوغها.

ب. تحليلُ البياناتِ بما يتناسبُ معَ الخبراتِ السابقةِ.

ج. استخدامُ الحوسبةِ السحابيةِ.

د. تحويلُ الأنشطةِ اليدويةِ إلى حاسوبيةٍ.

تقويم ذاتيٌّ (Self–Checklist)

بعدَ دراســـتي هذهِ الوَحْدةِ، اقرأُ الفقْراتِ الواردةَ في الجدولِ الآتي، ثمَّ أضعُ إشارةَ (✓) في العمودِ المناسبِ:

مؤشراتُ الأداءِ	نعمْ	لا	لسْتُ مُتأكِّدًا
أُعرِّفُ الذكاءَ الاصطناعيَّ.	○	○	○
أُعددُ أمثلةً على أنظمةِ الذكاءِ الاصطناعيِّ.	○	○	○
أُبينُ خصائصَ الذكاءِ الاصطناعيِّ.	○	○	○
أُميِّزُ أنظمةَ الذكاءِ الاصطناعيِّ.	○	○	○
أشرحُ مكوناتِ نظامِ الذكاءِ الاصطناعيِّ.	○	○	○
أشرحُ آليةَ عملِ نظامِ الذكاءِ الاصطناعيِّ.	○	○	○
أقارنُ بينَ أنظمةِ الذكاءِ الاصطناعيِّ والأنظمةِ التقليديةِ.	○	○	○
أُبينُ مراحلَ تطورِ الذكاءِ الاصطناعيِّ.	○	○	○
أُوضحُ طبيعةَ الأنظمةِ في كلِّ مرحلةٍ منْ مراحلِ الذكاءِ الاصطناعيِّ.	○	○	○
أشرحُ أهميةَ الذكاءِ الاصطناعيِّ.	○	○	○
أُوضحُ مجالاتِ تطبيقِ الذكاءِ الاصطناعيِّ في النُّظمِ المعرفيةِ الأخرى.	○	○	○
أُوضحُ تطبيقاتِ الذكاءِ الاصطناعيِّ.	○	○	○

مؤشراتُ الأداءِ	نعمْ	لا	لسْتُ مُتأكِّدًا
أُحدّدُ الآثارَ الاجتماعيةَ للذكاءَ الاصطناعيِّ.	○	○	○
أُعرّفُ نظامَ الروبوتِ.	○	○	○
أُوضّحُ أهميةَ نظامِ الروبوتِ.	○	○	○
أذكرُ استخداماتِ الروبوتِ.	○	○	○
أُبرمجُ الروبوتَ على الحركاتِ الأساسيةِ في بيئةٍ افتراضيةٍ لأداءِ مهمةٍ معينةٍ.	○	○	○

تعليماتٌ للمراجعةِ والتحسينِ:

إذا اخترْتُ (لا) أوْ (لسْتُ مُتأكِّدًا) لأيٍّ منَ الفقْراتِ السابقةِ، فأتَّبِعُ الخطواتِ الآتيةَ لتجنُّبِ ذلكَ:

- أُراجِعُ المادةَ الدراسيةَ؛ بأنْ أُعيدَ قراءةَ المحتوى المُتعلِّقِ بالمعيارِ.
- أطلبُ المساعدةَ؛ بأنْ أُناقِشَ مُعلِّمي/ مُعلِّمتي أوْ زملائي/ زميلاتي في ما تعذَّرَ عليَّ فهمُهُ.
- أستخدِمُ مراجعَ إضافيةٍ؛ بأنْ أبحثَ عنْ مراجعَ أُخرى مثلَ الكتبِ، أوْ أستعينَ بالمواقعِ الإلكترونيةِ الموثوقةِ التي تُقدِّمُ شرحًا وافيًا للموضوعاتِ التي أجدُ صعوبةً في فهمِها.

تأمُّلاتٌ ذاتيةٌ

عزيزي الطالبَ/ عزيزتي الطالبةَ:
التأمُّلاتُ الذاتيةُ هيَ فرصةٌ لتقييمِ عمليةِ التعلُّمِ، وفهمِ التحدِّياتِ، وتطويرِ استراتيجياتٍ لتحسينِ عمليةِ التعلُّمِ مستقبلًا. أملأُ الفراغَ في ما يأتي بالأفكارِ والتأمُّلاتِ الشخصيةِ التي يُمكِنُ بها تحقيقُ أفضلِ استفادةٍ منَ التجربةِ التعليميةِ:

تعلَّمْتُ في هذهِ الوحدةِ:

يُمكِنُني أنْ أُطبِّقَ ما تعلَّمْتُهُ في:

الصعوباتُ التي واجهْتُها أثناءَ عمليةِ التعلُّمِ:

ذلَّلْتُ هذهِ الصعوباتِ عنْ طريقِ:

يُمكِنُني مستقبلًا تحسينُ:

تم بحمد الله