المملكة العربية السعودية

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

وزارة التعليم
Ministry of Education

دليل المعلم

الأمن السيبراني
Cybersecurity

وزارة التعليم
Ministry of Education
2023 - 1445

binarylogic

السنة الثالثة
التعليم الثانوي - نظام المسارات

طبعة 2023-1445

الأمن السيبراني

السنة الثالثة - التعليم الثانوي - نظام المسارات

طبعة 2023-1445

رقم الإيداع : ١٤٤٥/٣٦٥٥
ردمك : ٩٧٨-٦٠٣-٥١١-٥٧٩-٧

التعليمية
TALEMIA

الاســم : ..... المدرسة : .....

المملكة العربية السعودية

وزارة التعليم
Ministry of Education

قررت وزارة التعليم تدريس
هذا الكتاب وطبعه على نفقتها

الأمن السيبراني

التعليم الثانوي - نظام المسارات

السنة الثالثة

دليل المعلم

طبعة 1445-2023

وزارة التعليم
Ministry of Education
2023 - 1445

فهرسة مكتبة الملك فهد الوطنية أثناء النشر
وزارة التعليم
دليل المعلم – الأمن السيبراني – التعليم الثانوي – نظام المسارات – السنة الثالثة. / وزارة التعليم . – Riyadh، ١٤٤٥ هـ
١١١ ص ؛ ٢١ x ٢٧.٥ سم
ردمك : ٧ – ٥٧٩ – ٥١١ – ٦٠٣ – ٩٧٨

رقم الإيداع : ١٤٤٥ / ٣٦٥٥
ردمك : ٧ - ٥٧٩ - ٥١١ - ٦٠٣ - ٩٧٨

www.moe.gov.sa

مواد إثرائية وداعمة على "منصة عين الإثرائية"

IEN.EDU.SA

تواصل بمقترحاتك لتطوير الكتاب المدرسي

FB.T4EDU.COM

وزارة التعليم
Ministry of Education
2023 - 1445

الناشر: شركة تطوير للخدمات التعليمية

تم النشر بموجب اتفاقية خاصة بين شركة Binary Logic SA وشركة تطوير للخدمات التعليمية
(عقد رقم 2021/0010) للاستخدام في المملكة العربية السعودية

binarylogic

وزارة التعليم
Ministry of Education
2023 - 1445

بسم الله الرحمن الرحيم

وزارة التعليم
Ministry of Education
2023 - 1445

الفهرس

نظرة عامة

وزارة التعليم
Ministry of Education
2023 - 1445

نظرة عامة على محتوى كتاب الأمن السيبراني للصف الثالث الثانوي

مقدمة

إن تقدم الدول وتطورها يقاس بمدى قدرتها على الاستثمار في التعليم، ومدى استجابة نظامها التعليمي لمتطلبات العصر ومتغيراته. وحرصًا من وزارة التعليم على ديمومة تطوير أنظمتها التعليمية، واستجابة لرؤية المملكة العربية السعودية 2030 فقد بادرت الوزارة إلى اعتماد نظام "مسارات التعليم الثانوي" بهدف إحداث تغيير فاعل وشامل في المرحلة الثانوية. ويتكون نظام المسارات من تسعة فصول دراسية تُدرّس في ثلاث سنوات، تتضمن سنة أولى مشتركة يتلقى فيها الطلبة الدروس في مجالات علمية وإنسانية متنوعة، تليها سنتان تخصصيتان يُسكّن الطلبة بها في مسار عام وأربعة مسارات تخصصية تتسق مع ميولهم وقدراتهم، وهي: المسار الشرعي، مسار إدارة الأعمال، مسار علوم الحاسب والهندسة، مسار الصحة والحياة. وبالتالي فإن مسار علوم الحاسب والهندسة كأحد المسارات المستحدثة في المرحلة الثانوية يسهم في تحقيق أفضل الممارسات عبر الاستثمار في رأس المال البشري، وتحويل الطالب إلى فرد مشارك ومنتج للعلوم والمعارف، مع إكسابه المهارات والخبرات اللازمة لاستكمال دراسته في تخصصات تتناسب مع ميوله وقدراته أو الالتحاق بسوق العمل. وتعدُّ مادة الأمن السيبراني أحد المواد الرئيسة في مسار علوم الحاسب والهندسة التي تقدم في كتاب شامل، حيث تسهم في توضيح مفاهيم الأمن السيبراني والتقنيات المرتبطة به، وذلك مع التركيز بشكل خاص على التهديدات السيبرانية واستراتيجيات الحد منها. وتهدف المادة إلى تعريف الطالب بأهمية الأمن السيبراني في مختلف الصناعات، والقطاعات المالية، ومؤسسات الرعاية الصحية، والهيئات الحكومية، كما تغطي أساسيات الأمن السيبراني بما في ذلك تقييم المخاطر، وأمن البرمجيات والشبكات والاستجابة للحوادث، ويوفر الكتاب تمارين عملية لتعزيز فهم الطالب لمفهوم التشفير، كما يؤكد الكتاب على أهمية توعية المستخدم، والكشف الاستباقي عن التهديدات، واستخدام الأدوات الرقمية في حماية الأفراد والمنظمات. ويتميز كتاب الأمن السيبراني بأساليب حديثة، تتوافر فيه عناصر الجذب والتشويق، والتي تجعل الطلبة يقبلون على تعلمه والتفاعل معه، من خلال ما يقدمه من تدريبات وأنشطة متنوعة، كما يؤكد هذا الكتاب على جوانب مهمة في تعليم الأمن السيبراني وتعلمه، تتمثل في:

- الترابط الوثيق بين المحتويات والتهديدات السيبرانية الواقعية.
- تنوع طرائق عرض المحتوى بصورة جذابة ومشوقة.
- إبراز دور المتعلم في عمليات التعليم والتعلم.
- الاهتمام بترابط محتوياته مما يجعل منه كلًا متكاملًا.

وزارة التعليم
Ministry of Education
2023 - 1445

- الاهتمام بتوظيف التقنيات المناسبة في المواقف المختلفة.

- الاهتمام بتوظيف أساليب متنوعة في تقويم الطلبة بما يتناسب مع الفروق الفردية بينهم.

ولمواكبة التطورات العالمية في هذا المجال، فإن دليل مادة الأمن السيبراني يوفر للمعلّم مجموعة متكاملة من المواد التعليمية المتنوعة التي تراعي الفروق الفردية بين الطلبة، بالإضافة إلى البرمجيات والمواقع التعليمية التي توفر للطلبة فرصة توظيف التقنيات الحديثة والتواصل المبني على الممارسة.

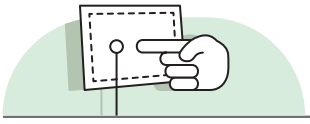
ويأتي هذا الدليل عونًا لمعلّمي ومعلّمات مقرر "الأمن السيبراني" في تحقيق الأهداف التعليمية والتربوية المستهدفة من المقرر، من خلال التركيز على تقديم مقترحات إجرائية تساعد المعلّم والمعلّمة على تقديم الدروس للمتعلمين بكفاءة عالية، وتوفير مادة إثرائية لمحتوى الدروس؛ لتمكين المعلّم من تقديم موضوعات الكتاب بشكل أفضل، مع الأخذ في الاعتبار أن الأساليب والتوجيهات الواردة ليست سوى مقترحات معينة، وللمعلّم والمعلّمة اختيار ما يلائم الموقف التعليمي والإمكانات المتاحة، بالإضافة إلى مراعاة حاجات المتعلمين، واهتماماتهم، وقدراتهم، والتي يمكن أن تتطلب الابتكار والإبداع، لتهيئة بيئة التعلم المناسبة.

وفي الختام نسأل الله العلي القدير أن يكون هذا الدليل عونًا للمعلّمين والمعلّمات، لتقديم رسالتهم الجليلة، وأداء مهمتهم على النحو المنشود.

والله ولي التوفيق

الإستراتيجيات التعليمية

هناك العديد من الإستراتيجيات التعليمية التي يمكن استخدامها أثناء الدرس، وقد صُمّم كتاب الطالب بهذه الطريقة لمساعدتك في تطبيق بعض هذه الإستراتيجيات في الأجزاء النظرية والعملية من الدرس. يمكنك أن ترى في القسم التالي بعض أمثلة الإستراتيجيات التعليمية التي تستطيع استخدامها.



التعليم المباشر (المحاضرة)

يُعدُّ التعليم المباشر في هذه المرحلة العمرية الأكثر فاعلية وكفاءة عند تدريس فكرة أو مهارة.

أمثلة

> يمكن استخدام إستراتيجية التعليم المباشر لإرشاد الطلبة إلى معرفة مفاهيم الأمن السيبراني.

الأمن السيبراني | كتاب الطالب | صفحة 9

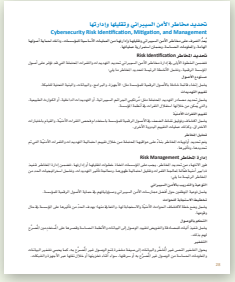
وزارة التعليم
Ministry of Education
2023 - 1445

التعلُّم القائم على حل المشكلات

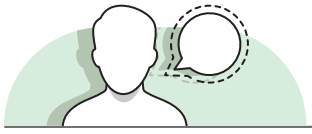
تعتمد إستراتيجية حل المشكلات على تقديم عدة حلول مختلفة لمشكلة واحدة، والهدف ليس الحصول على إجابة واحدة صحيحة كما هو الحال مع الاستكشاف الموجه، وإنما الحصول على أكبر عدد ممكن من الحلول المختلفة للتحدي المطروح أمام الطلبة.

أمثلة

> يمكن استخدام إستراتيجية التعلُّم القائم على حل المشكلات أثناء تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها.



الأمن السيبراني | كتاب الطالب | صفحة 28



إستراتيجية المناقشة والحوار

تتيح إستراتيجية التدريس المبنيَّة على إدارة المناقشات فرصةً لتحفيز التفكير الناقد، وتُعدُّ الأسئلة المتكررة (سواء من المعلّم أو من الطلبة) وسيلةً لقياس التعلم والاستكشاف العميق للمفاهيم الأساسية الخاصة بالمنهج.

أمثلة

> يمكن استخدام إستراتيجية المناقشة والحوار أثناء تعليم الطلبة الجوانب الموضوعية المتعلقة بالقرصنة الأخلاقية.

الأمن السيبراني | كتاب الطالب | صفحة 45

وزارة التعليم
Ministry of Education
2023 - 1445

الاستقصاء أو الاستكشاف

تتيح هذه الإستراتيجية للطلبة بناء المعرفة بمفردهم من خلال المرور بعمليات مختلفة أو تجارب أو إجراء التحقق والاستبعاد.

أمثلة

> يمكن استخدام إستراتيجية الاستكشاف في تمرينات متنوعة تتطلب من الطلبة إجراء بحث على الشبكة العنكبوتية وجمع المعلومات لإكمال التمرين.

الأمن السيبراني | كتاب الطالب | صفحة 99

التعلُّم القائم على المشروع

يمكن تنفيذ الأنشطة القائمة على المشروعات بصورة مُستقلة أو في إطار تعاوني، ويكون دور المُعلِّم هو تقديم التوجيه والإرشاد للطلبة من أجل إكمال مشروعاتهم بنجاح، واكتساب فهم عميق للمفاهيم الأساسية.

أمثلة

> في نهاية كل وحدة يمكن للطلبة تطبيق جميع المهارات التي تعلموها من خلال إكمال المشروع باستخدام إستراتيجية التعلُّم القائم على المشروع.

الأمن السيبراني | كتاب الطالب | صفحة 100

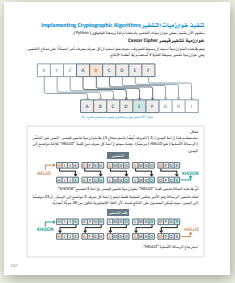
وزارة التعليم
Ministry of Education
2023 - 1445

التعلُّم التعاوني

يُعدُّ التعلُّم التعاوني إستراتيجية تعليمية فعالة تُنفذ من خلال فرق عمل صغيرة، يتكون كل منها من طلبة من مستويات متفاوته في القدرات، ويتمُّ من خلال العملية التربوية تقديم مجموعة متنوعة من الأنشطة التعليمية لتحسين استيعابهم لمفهوم ما وممارسة مهاراتهم.

أمثلة

> يمكن للطلبة التعاون في مجموعات لإكمال المشروعات والتمرينات، على سبيل المثال: يمكنهم التعاون لفك التشفير، واختباره لرسالة ما.



الأمن السيبراني | كتاب الطالب | صفحة 117

إستراتيجيات التقويم

التقويم التشخيصي

يتم تطبيق التقويم التشخيصي قبل البدء في الدرس، وعادة ما يأخذ شكل الاختبارات التمهيدية التي تعمل كمؤشر لقياس المعلومات التي يعرفها الطلبة عن موضوع ما.

تعدّ هذه الاختبارات التمهيدية مفيدة للمعلّم (وكذلك الطلبة) لأنها تخبره بمدى معرفتهم بموضوع الدرس، مما يساعده على التخطيط بطريقة أفضل للدرس وتحديد أهداف التعلُّم ومعرفة النقاط التي تحتاج إلى شرح أكثر والعكس.

من الفوائد الأخرى للتقويم التشخيصي إعطاء الطلبة فكرة عما سيتعلموه في نهاية الدرس أو الوحدة وعند دمجه مع التقويم الختامي، يتضح مقدار المعارف والمهارات التي اكتسبوها. ويوفر بيانات مهمة حول تقدم الطلبة على مدار العام.

فيما يلي نلخّص بعض النقاط المهمة حول التقويم التشخيصي وهي:

- تطبيقه قبل بداية الوحدة أو الدرس.
- يهدف إلى تحديد المعرفة الحالية للطلبة.
- تحديد النقاط التي يحتاج فيها الطلبة إلى فهم أكثر.
- تحديد احتياجات الطلبة.
- معرفة الفروق الفردية بين الطلبة.
- بناء مهارة التقدير لدى الطلبة ومساعدتهم على إدراك مدى تقدمهم.
- لا يمثل ضغط على الطلبة (حيث لا يعتد به في الدرجة النهائية).

التقويم التكويني

التقويم التكويني هو تقويم لأجل التعلُّم وليس من أجل الدَّرجات أو لإصدار الشهادات (مثل التقويم الختامي). يساعد التقويم التكويني كلًّا من الطالب والمعلّم على فهم نقاط الضعف المحتملة ورفع المستوى العلمي.

الغرض من التقويم التكويني هو تزويد الطلبة بالتغذية الراجعة البناءة حول عملهم؛ لتعزيز عملية التعلُّم. وتساعد الملحوظات السريعة أثناء تعلُّم الطلبة للمواد التعليمية على توضيح الأفكار وتصحيح المفاهيم الخطأ في مرحلة مبكرة، ومن المهم تقديم التغذية الراجعة البناءة بشكل مكثف ومستمر وفوري أثناء تعلُّم الطلبة لتحقيق نتائج جيدة.

يُنفذ هذا النوع من التقويم أثناء الدرس بعد إكمال كل جزئية منه، ويُنصَحُ في بعض الأحيان باستخدام الأسئلة الشفوية المختارة بعناية والموجهة جيدًا لفاعليتها الكبيرة في التقويم التكويني.

بعض النقاط الأساسية التي يجيب عنها التقويم التكويني:

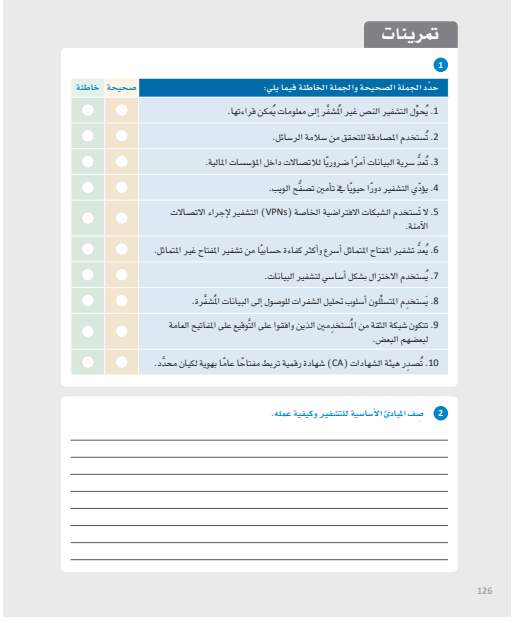
- هل يفهم الطالب المصطلحات والمبادئ الأساسية؟ هل هناك طريقة أفضل للتعامل مع المشكلة؟
- يمكن أن تتضمن المهام التكوينية في الدروس التمهيدية أحيانًا تدريبات أو مهام قصيرة نسبيًا، للسماح للطلبة بترسيخ المفاهيم الأساسية واكتساب الممارسة الأولية.

ضع في الاعتبار أنه يمكن استخدام التمارين القصيرة (الاختيار من متعدد، ملء الفراغات، ونحوها) أثناء الدرس لتقويم فهم الطلبة وتقدمهم وتصحيح الأخطاء. مثل هذه التمارين متوفرة في جميع الدروس تقريبًا في كتاب الطالب.

مثال التقويم التكويني (تقويم تطور الطلبة)

المرحلة الثانوية - نظام المسارات (السنة الثالثة)

ص. 126



تمرينات

1

حدد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُحوِّل التشفير النص غير المُشفَّر إلى معلومات يُمكن قراءتها.		
2. تُستخدم المصادقة للتحقق من سلامة الرسائل.		
3. تُعدُّ سرية البيانات أمرًا ضروريًا للاتصالات داخل المؤسسات المالية.		
4. يؤدي التشفير دورًا حيويًا في تأمين تصفُّح الويب.		
5. لا تستخدم الشبكات الافتراضية الخاصة (VPNs) التشفير لإجراء الاتصالات الآمنة.		
6. يُعدُّ تشفير المفتاح المتماثل أسرع وأكثر كفاءة حسابيًا من تشفير المفتاح غير المتماثل.		
7. يُستخدم الاختزال بشكل أساسي لتشفير البيانات.		
8. يَستخدِم المتسلِّلون أسلوب تحليل الشفرات للوصول إلى البيانات المُشفَّرة.		
9. تتكون شبكة الثقة من المُستخدِمين الذين وافقوا على التَّوقيع على المفاتيح العامة لبعضهم البعض.		
10. تُصدِر هيئة الشهادات (CA) شهادة رقمية تربط مفتاحًا عامًا بهوية لكيان محدَّد.		

2 صف المبادئ الأساسية للتشفير وكيفية عمله.

126

التقويم الختامي (النهائي)

على عكس التقويم التكويني، فإن هدف التقويم النهائي هو تحديد درجة/مدى الإتقان ومنح الدرجات. وعادةً ما يطبق هذا النوع من التقويم مرات قليلة في الفصل الدراسي (مثل الاختبارات الفصلية وبعض المشروعات) أو الاختبار النهائي.

> بعض النقاط الأساسية التي يجيب عنها التقويم النهائي:

- إلى أي مدى أتقن الطالب؟ ما مدى صحة إجابة الطالب أو حل مشكلة أو هل نفذ مشروعًا عمليًا؟ كيف ترتبط جودة هذا العمل بالتوقُّع المعياري؟
- مستوى الفهم من خلال الدرجة الكلية للطالب.

> الأمور التي يحتاج المعلّم مراعاتها في الاختبارات هي:

- الوقت المتاح لإتمام المهام العملية في الاختبار، وخاصة للطلبة الذين يحتاجون وقتًا أطول من متوسط الطلبة الآخرين.
- أن تكون معايير التقويم وما يتوقع من الطلبة تقديمه أثناء الاختبار واضحةً وموجزةً.
- توفير الأدوات البرمجية المطلوبة لكل اختبار والحلول للأعطال المحتملة غير المتوقعة أو أعطال الأجهزة.
- الإعداد السليم لمعمل الحاسب والمستندات المطلوبة للجزء العملي من الاختبار.

ضع في الحسبان ضرورة تواجد مساعد أثناء إجراء الاختبارات في معمل الحاسب. قم بإجراء الاختبار بنفسك للتأكد من عدم وجود مشكلات غير متوقعة في الأجهزة أو البرامج. قم بتحديد الوقت الذي تحتاجه لإكمال الاختبار وفق الفئة العمرية ومهارات الطلبة العملية.

تعدُّ المشروعات من أدوات التقويم النهائي، وهي ليست تمارين قصيرة أو أسئلة ذات إجابة محددة مسبقًا، فربما يخرج جميع الطلبة بنتائج مختلفة للمشروع ولكن كلها صحيحة. مما يعني أن تقويم المشروع يجب أن يتَّبِع استراتيجية معينة من شأنها تقويم عمل الطلبة بناءً على معايير محددة مسبقًا مثل: المعرفة والمهارات والإبداع والهدف من المشروع. فعلى سبيل المثال، يمكن استخدام نشاط المشروع لتقييم فهم الطلبة وتقدمهم في إنشاء تقرير يقيم مدى جاهزية المؤسسة للأمن السيبراني. حيث يمكن لجميع الطلبة تقديم نتيجة نهائية للمشروع، لكن بعض النتائج قد تكون أكثر إبداعًا، وبعضها له نتائج فنية أكثر أو بُنْيَة أفضل. قد تتضمن بعض مشروعات الطلبة المزيد من المهارات التي يتم تدريسها في الوحدة، وبالتالي تمثل إتقانًا أكثر للمحتوى التعليمي. وبطبيعة الحال يمكن أن تلعب العديد من العوامل دورًا مهمًا في تقويم المشروع اعتمادًا على الفئة العمرية والموضوع الرئيس للوحدة. يأخذ المعلّم بعين الاعتبار الأهداف والغايات والنتائج المرجوة للدرس، ومدى تعقيد أو تحديات المشروع لتحديد معايير التقويم الخاصة به.

معايير تقييم مشروع وفق سلالم التقدير

الجدول أدناه يُعد مثالًا على بناء سُلّم تقدير لتقييم مشروع معين:

	غير مقبول	مقبول	جيد	ممتاز
المعرفة	لم تُطبق المعرفة المطلوبة	تم تطبيق جزء من المعرفة المطلوبة	تم تطبيق كل المعرفة المطلوبة	تم تطبيق المعرفة من مختلف المجالات / المستويات
المهارات	لم تُطبق المهارات المطلوبة	تم تطبيق جزء من المهارات المطلوبة	تم تطبيق جميع المهارات المطلوبة	تم تطبيق المهارات من مختلف المجالات / المستويات
الإبداع	لم يتم تسليم المشروع	المشروع لم يكن مميزًا	المشروع مميز	يتضمن المشروع أفكارًا إبداعية
الدقة	المشروع يحتوى على الكثير من الأخطاء	المشروع يحتوي على أخطاء متوسطة	المشروع يحتوي على أخطاء بسيطة	المشروع خالٍ من الأخطاء
تحقق الأهداف	لم يتم تحقيق جميع أهداف المشروع	لم يتم تحقيق غالبية أهداف المشروع	تم تحقيق غالبية أهداف المشروع	تم تحقيق جميع أهداف المشروع

يجب أن يكون الطلبة على دراية بمعايير التقويم وما هو متوقع منهم، وأن يتلقوا تغذية راجعة مفصلة حول تقويم مشروعاتهم؛ للتأكد من فهمهم الكامل لنقاط الضعف وكيف يمكنهم تحسينها في مشروعاتهم المستقبلية.

تلميح: يعتبر سُلّم التقدير أعلاه عام، حيث أن بعض مستويات الأداء تتضمن وصفًا يحتاج إلى تفصيل وفقًا لطبيعة ومتطلبات المشروع.

عدد الساعات الدراسية لكل درس

الوحدة الأولى : أساسيات الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: مقدمة في الأمن السيبراني	2
الدرس الثاني: مخاطر الأمن السيبراني وثغراته	3
الدرس الثالث: تهديدات الأمن السيبراني وضوابطه	3
المشروع	3
إجمالي عدد حصص الوحدة الأولى	**11**
الوحدة الثانية : الحماية والاستجابة في الأمن السيبراني	**عدد الحصص الدراسية**
الدرس الأول: أمن العتاد والبرمجيات ونظام التشغيل	4
الدرس الثاني: أمن الشبكات والويب	4
الدرس الثالث: التحليل الجنائي الرقمي والاستجابة للحوادث	4
المشروع	3
إجمالي عدد حصص الوحدة الثانية	**15**
الوحدة الثالثة : مواضيع متقدِّمة في الأمن السيبراني	**عدد الحصص الدراسية**
الدرس الأول: تشريعات وقوانين الأمن السيبراني	1
الدرس الثاني: التشفير في الأمن السيبراني	3
الدرس الثالث: الأمن السيبراني والتقنيات الناشئة	3
المشروع	3
إجمالي عدد حصص الوحدة الثالثة	**10**
إجمالي عدد حصص جميع الوحدات	**36**

الوحدة الأولى

أساسيات الأمن السيبراني

وصف الوحدة

عزيزي المعلّم

الغرض العام من الوحدة هو أن يتعرف الطلبة على المفاهيم الأساسية للأمن السيبراني، ومراحل تطوره، والدور الذي يلعبه في العالم المعاصر، بالإضافة إلى التعرّف على المخاطر والثغرات الأمنيّة الموجودة في الأنظمة التقنية، وعلى استراتيجيات الاستجابة لتلك المخاطر ومواجهتها، كما سيتعرفوا على **حماية البيانات** (Data Protection) في الأمن السيبراني، و**التحكم بالوصول** (Access Control) لحماية أنظمة المعلومات، وكذلك دور **القرصنة الأخلاقية** (Ethical Hacking) في حماية المؤسسات والشركات.

أهداف التعلُّم

- توضيح المقصود بمجال الأمن السيبراني وتاريخه.
- تعداد المبادئ الأساسية للأمن السيبراني.
- تحليل الأدوار الوظيفية الرئيسة في الأمن السيبراني.
- معرفة النشأة الرائدة للمملكة العربية السعودية في مجال الأمن السيبراني.
- تعداد الفئات المختلفة للبرمجيات الضارة.
- توضيح كيفية عمل الهجمات السيبرانية.
- تقييم الاستراتيجيات المختلفة لتحديد المخاطر وكيفية الحدّ منها وإدارتها.
- تحديد كيفية مساعدة تقنيات التحكم بالوصول في حماية أنظمة المعلومات.
- شرح دور القرصنة الأخلاقية في مجال الأمن السيبراني.

الدروس	
الوحدة الأولى: أساسيات الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: مقدمة في الأمن السيبراني	2
الدرس الثاني: مخاطر الأمن السيبراني وثغراته	3
الدرس الثالث: تهديدات الأمن السيبراني وضوابطه	3
المشروع	3
إجمالي عدد حصص الوحدة الأولى	11

المصادر والملفات والأدوات والأجهزة المطلوبة

المصادر

كتاب الأمن السيبراني

التعليم الثانوي – نظام المسارات

السنة الثالثة

الملفات الرقمية

يُمكنك الوصول للحلول أو الملفات النهائية للتمرينات التي يمكن استخدامها على منصة "عين" الإثرائية، وهي:

> مجلد G12.CYB.S3.U1

مقدمة في الأمن السيبراني

وصف الدرس

الهدف العام من الدرس هو التعرف على مفهوم الأمن السيبراني، وتاريخه، ومبادئه الأساسية، والأدوار الوظيفية فيه، بالإضافة إلى معرفة نشأة الأمن السيبراني في المملكة العربية السعودية والمبادرات المهنية له.

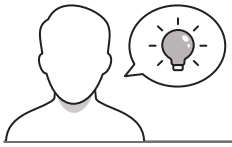
أهداف التعلُّم

- توضيح المقصود بالأمن السيبراني وتاريخه.
- معرفة المبادئ الأساسية للأمن السيبراني.
- معرفة الأدوار الوظيفية في الأمن السيبراني.
- معرفة نشأة الأمن السيبراني في المملكة العربية السعودية والمبادرات المهنية له.

الدرس الأول	
الوحدة الأولى: أساسيات الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: مقدمة في الأمن السيبراني	2

نقاط مهمَّة

- قد يظن بعض الطلبة أن الأمن السيبراني بدأ في العقود القليلة الماضية، وضّح لهم أنه يعود للسبعينات من القرن العشرين، ولكن التعليم والتوعية بمجال الأمن السيبراني انتشرت في السنوات الماضية لتزايد الهجمات السيبرانية وتعقيدها.
- قد لا يدرك بعض الطلبة الفرق بين تهديدات الأمن السيبراني والهجمات السيبرانية، وضّح لهم الفرق بينهما، وقدّم الأمثلة على كل منهما.

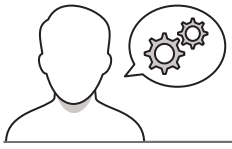


التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- ماذا نقصد بالأمن السيبراني؟
- هل تعرفون تاريخ بدء الأمن السيبراني على مستوى العالم؟
- ما الجهات الحكومية المختصة بالأمن السيبراني في المملكة العربية السعودية؟



خطوات تنفيذ الدرس

> في البداية ناقِش الطلبة حول مفهومهم عن الأمن السيبراني، واطلب منهم تقديم الأمثلة عليه.

> وضّح لهم مفهوم الأمن السيبراني وتعريفه حسب تنظيم **الهيئة الوطنية للأمن السيبراني** (National Cybersecurity Authority - NCA).

> بعد ذلك، اشرح لهم أهمية الأمن السيبراني للأفراد والمنظمات والحكومات.

> وضّح لهم الفرق بين تهديدات الأمن السيبراني، والهجمات السيبرانية.

> اطلب منهم حل التمرين الثاني؛ للتحقق من إدراكهم لمفهوم الأمن السيبراني.

> انتقل إلى توضيح تاريخ الأمن السيبراني، ووضّح لهم الحقبة الزمنية التي يعود لها مفهوم الأمن السيبراني.

> قدّم لهم الأسباب التي أدت لتطور مفهوم الأمن السيبراني، والأمثلة على أبرز الهجمات السيبرانية التي عرَّضت الحكومات والشركات والأفراد للخطر.


الدرس الأول
مقدمة في الأمن السيبراني

ما المقصود بالأمن السيبراني؟ What is Cybersecurity

أصبح مجال الأمن السيبراني مهمًا بشكل متزايد في السنوات الأخيرة، خاصةً مع الاندماج الكبير للتقنية في الحياة اليومية؛ فمع ظهور الإنترنت وانتشار أجهزة الحاسب والأجهزة المحمولة، أصبح الأمن السيبراني ضروريًا لحماية المعلومات الحساسة وضمان حماية الأنشطة عبر الإنترنت وأمنها، حيث يشمل مجال الأمن السيبراني مجموعة من الممارسات والتقنيات المصممة لحماية من التهديدات والهجمات السيبرانية.

تأسست الهيئة الوطنية للأمن السيبراني (National Cybersecurity Authority - NCA) في المملكة العربية السعودية بموجب أمر ملكي، وذلك كجهة مختصة بالأمن السيبراني، والمرجع الوطني في شؤونه، حيث يتم تعريف الأمن السيبراني حسب تنظيم الهيئة الوطنية للأمن السيبراني كما يلي:

هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

تهديدات الأمن السيبراني (Cybersecurity Threats):

تمثّل هذه التهديدات في أيّ ظرف أو حدث قد يؤثر سلبًا على العمليات، أو الأصول التنظيمية، أو الأفراد من خلال نظام معلومات عبر الوصول غير المصرّح به، أو التخريب والإفصاح عن المعلومات وتغييرها، أو حجب الخدمة.

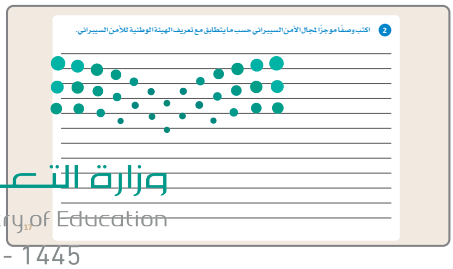
الهجمات السيبرانية (Cybersecurity Attacks):

هي إجراء يقوم به طرف ممّن ذو نوايا سيئة بهدف الإتلاف، أو التعطيل، أو الوصول غير المصرّح به إلى أنظمة الحاسب أو الشبكات أو البيانات.

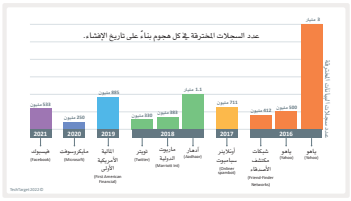
تمثّل الطبيعة المتطورة والمتغيّرة للتهديدات السيبرانية التحدي الرئيس للأمن السيبراني، حيث يتغيّر هذا المجال بشكل مستمر، ولذلك يحتاج المختصون إلى تطوير إجراءاتهم الأمنية بأستمرار لمواكبة هذه التغيرات. ويتضمن الأمن السيبراني مجالات مختلفة مثل أمن البيانات، وأمن الشبكات، والتشفير، وإدارة المخاطر السيبرانية. وبسبب طبيعة مجال الأمن السيبراني الذي يشمل عددًا من التخصصات البينية فإن العمل فيه يُعدّ تحديًا مثيرًا لتقديمه العديد من فُرص التعلّم والتقدم الوظيفي.

تُعدُّ حماية البيانات والمعلومات أمرًا ضروريًا. وكذلك تدابير الأمن السيبراني ضرورية للحماية من الهجمات السيبرانية. فقد تتعرض البيانات الشخصية والمعلومات المالية والملكية الفكرية للخطر بسبب هذه الهجمات، وقد تكون العواقب الناجمة عن أي هجوم سيبراني ناجح وخيمة للغاية. وبشكل خاص عند تسببها بخسائر مالية للأفراد، حيث تؤدي أغلب الهجمات السيبرانية الناجحة إلى سرقة الأموال أو الأصول

9


٢ اكتب وصفًا موجزًا لمجال الأمن السيبراني حسب ما يتطابق مع تعريف الهيئة الوطنية للأمن السيبراني.

- انتقِل إلى شرح المبادئ الأساسية للأمن السيبراني، ووضّح لهم المقصود بمثلث أمن المعلومات (CIA Triad): السرية (Confidentiality) والسلامة (Integrity) والتوافر (Availability).
- وجّه الطلبة لحل التمرينات الثالث والرابع والخامس؛ للتحقق من فهمهم للمبادئ الأساسية للأمن السيبراني.
- اشرح الأدوار الوظيفية في الأمن السيبراني، ووضّح لهم حجم فرص العمل في هذا المجال.
- يمكنك بعدها تقسيم الطلبة لمجموعات متكافئة، ثم اطلب من كل مجموعة كتابة أبرز الأدوار الوظيفية ومجالاتها وفئاتها الواردة في تصنيف السعودي لكوادر الأمن السيبراني (سيوف) (Saudi Cybersecurity Workforce Framework – SCyWF) وناقِش إجاباتهم، ثم قدّم التغذية الراجعة لهم.



شكل 1.2: مثلوم من أكبر خروقات البيانات في التاريخ بناءً على عدد الملايين (TechTarget)

المبادئ الأساسية للأمن السيبراني Key Principles of Cybersecurity

تُعدُّ حماية أنظمة الحاسب والشبكات والبيانات من الوصول غير المُصرَّح به والأنشطة الضارة أمرًا بالغ الأهمية. فمن الضروري الالتزام بالمبادئ الأساسية للأمن السيبراني لإنشاء إطار أمني قوي وفعّال. كما يُعدُّ فهم هذه المبادئ وتنفيذها أمرًا حيويًا لحماية المعلومات الحساسة. وضمان دقة البيانات. والحفاظ على الوصول غير المنقطع إلى الموارد الهامة.

فيما يلي عرض لهذه المبادئ الأساسية:

السرية والسلامة والتوافر (مثلث أمن المعلومات)
Confidentiality, Integrity, and Availability (The CIA Triad)

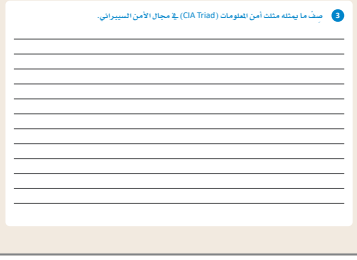
مثلث أمن المعلومات (The CIA Triad) هو نموذج يُستخدم على نطاق واسع لتصميم سياسات وممارسات الأمن السيبراني وتنفيذها. حيث يشير الاختصار CIA إلى السرية (Confidentiality – C) والسلامة (Integrity – I) والتوافر (Availability – A). وهي الأهداف الرئيسة الثلاثة لحماية المعلومات والأنظمة من الوصول غير المصرَّح به أو التغيير أو الانقطاع.

شكل 3.1: مثلث أمن المعلومات

تشير السرية (Confidentiality) إلى الحفاظ على القيود المُصرَّح بها للوصول إلى المعلومات، أي عدم السماح بالوصول للبيانات لمن لا يحق لهم الوصول إليها. ويُمكن الحفاظ على السرية من خلال طرائق مختلفة مثل: التشفير، والتحكم في الوصول، وإخفاء البيانات. وتواجه السرية تهديدات محتملة مثل: هجمات التصيد الإلكتروني. حيث ينتحل المهاجمون شخصيات كيانات شرعية لخداع الأفراد والحصول على معلومات حساسة.

تشير السلامة (Integrity) إلى توكيد دقة البيانات وعدم التلاعب بها. حيث إن سلامة البيانات ضرورية للحفاظ على الثقة في أنظمة المعلومات. فبدونها لا يُمكن للمُستخدمين الوثوق بدقة المعلومات التي يتلقونها. ويُمكن أن تساعد إجراءات

11


3 صف ما يمثله مثلث أمن المعلومات (CIA Triad) في مجال الأمن السيبراني.

17


4 وضّح كيف تساعد السرية في حماية المعلومات الحساسة.

5 اشرح سبب أهمية التوافر لضمان إمكانية وصول المُستخدمين إلى الأنظمة والخدمات.

18

- انتقل إلى شرح نشأة الأمن السيبراني في المملكة العربية السعودية وواقعه، ثم بيّن لهم المستوى العالمي والمراكز التي حققتها المملكة في مجال الأمن السيبراني.
- وضّح للطلبة أهم الجهات الحكومية التي تهتم بمجال الأمن السيبراني، واختصاص كلٍّ منها مثل: **الهيئة الوطنية للأمن السيبراني (NCA)**، و**الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز (SAFCSP)**.
- اشرح المبادرات المهنية للأمن السيبراني في المملكة العربية السعودية، وبيّن كيف أسهم ذلك في توفير وظائف وخبرات الأمن السيبراني في البلاد، ثم وضّح حجم فرص العمل في هذا المجال.
- وجّه الطلبة لحل التمرينين السادس والسابع؛ للتحقق من فهمهم لجهود المملكة العربية السعودية في مجال الأمن السيبراني.
- في الختام يمكنك توجيه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.

المبادرات المهنية للأمن السيبراني في المملكة العربية السعودية
Cybersecurity Career Initiatives in Saudi Arabia

تتخذ المملكة العربية السعودية خطوات مهمة لتلبية الحاجة إلى وظائف وخبرات الأمن السيبراني في البلاد. وتستعرض فيما يلي مبادرات المملكة في هذا المجال.

التعليم والتدريب

استثمرت الحكومة السعودية بشكل كبير في مجال برامج التعليم والتدريب في الأمن السيبراني لتطوير القدرات المحلية. حيث تضم العديد من الجامعات والمعاهد في المملكة العربية السعودية برامج متخصصة للحصول على درجات علمية وشهادات في هذا المجال. كما أطلقت الحكومة مبادرات تدريبية لتطوير مهارات متخصصي تقنية المعلومات في مجال الأمن السيبراني. ومن الأمثلة على هذه البرامج: برامج الأكاديمية الوطنية للأمن السيبراني التي لها العديد من المسارات، وتهدف إلى تطوير وبناء القدرات الوطنية في هذا المجال. وتوفير محتوى التدريب في مجالات الأمن السيبراني. ويوفر الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز (SAFCSP) معسكرات تدريبية ومسابقات في مجال الأمن السيبراني. كما أصدرت الهيئة الوطنية للأمن السيبراني (NCA) الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم) (Saudi Cybersecurity Higher Education Framework – SCyber_Edu) بهدف ضمان جودة التعليم العالي للأمن السيبراني في المملكة العربية السعودية. ويحدّد هذا الإطار الحد الأدنى من المتطلبات لبرامج التعليم العالي في هذا المجال لضمان مواءمة نتائج التعلّم مع الاحتياجات الوطنية للقوى العاملة في مجال الأمن السيبراني.

استراتيجية الأمن السيبراني

طوّرت المملكة العربية السعودية استراتيجية وطنية شاملة للأمن السيبراني تحدّد رؤية المملكة وأهدافها في هذا المجال. وتتضمن تلك الاستراتيجية خُطمًا لتطوير القدرات الوطنية للأمن السيبراني داخل المملكة، بالإضافة إلى تدابير لحماية البنية التحتية الحيوية وتعزيز التعاون الدولي في هذا المجال.

الشراكات الصناعية

تعمل الحكومة السعودية أيضًا بشكل وثيق مع شركات القطاع الخاص لتلبية الحاجة إلى الخبرات في مجال الأمن السيبراني. فعلى سبيل المثال: دخلت الحكومة في شراكة مع شركات دولية لتوفير برامج التدريب والتطوير لمتخصصي الأمن السيبراني.

تطوير قطاع الأمن السيبراني

لدى المملكة العربية السعودية العديد من المبادرات لتسريع تطوير قطاع الأمن السيبراني ونموه وبناء قدراته في المملكة، وتشمل هذه المبادرات البرنامج الوطني سايبرك (CyberIC) الذي يُعدُّ مظلة للعديد من المبادرات مثل: التمارين الوطنية السيبرانية (National Cyber Drills)، ومبادرات التدريب على الأمن السيبراني التي تستهدف فئات مختلفة من المجتمع. وتحديات الأمن السيبراني لتشجيع الابتكار وريادة الأعمال في هذا المجال. وكذلك لتشجيع منظومة القدرات المحلية في الأمن السيبراني وربط الشركات الناشئة في تقنيات الأمن السيبراني بالمستثمرين.

15

6 حلّل المبادرات المهنية الرئيسة لمجال الأمن السيبراني في المملكة العربية السعودية.

7 اشرح كيف أصبحت المملكة العربية السعودية واحدة من الدول الرائدة في تطوير أنظمة الأمن السيبراني وتشريعاته.

19

تمرينات

1

حدد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. تم تطوير مُدمّرات الحماية والتشفير لمكافحة الهجمات السيبرانية المتزايدة.	○	○
2. تُعدُّ الوكالات الحكومية من الأهداف الرئيسة للهجمات السيبرانية.	○	○
3. جميع الجرائم الإلكترونية لها نفس المستوى من الخطورة والعواقب.	○	○
4. السرية والسلامة والمصادقة تُدعّم ملكية أمن المعلومات.	○	○
5. الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز هو مؤسسة وطنية تهدف إلى تدريب المواهب المحلية في مجال الذكاء الاصطناعي.	○	○
6. تشير السلامة إلى التأكد من دقة البيانات وعدم التلاعب بها.	○	○
7. يُعدُّ التشفير والتحكم في الوصول وإخفاء البيانات من الطرائق المستخدمة للحفاظ على سرية البيانات.	○	○
8. تضمن السرية أن البيانات دقيقة ولم يتم التلاعب بها.	○	○
9. يُعدُّ رئيس إدارة الأمن السيبراني (CISO) مسؤولًا تنفيذيًا يشرف على برنامج الأمن السيبراني لمؤسسة معيّنة.	○	○
10. يؤدّي رئيس إدارة الأمن السيبراني دورًا وظيفيًا في الأمن السيبراني.	○	○

16

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. تم تطوير جُدران الحماية والتشفير لمكافحة الهجمات السيبرانية المتزايدة.	✓	
2. تُعدُّ الوكالات الحكومية من الأهداف الرئيسة للهجمات السيبرانية.	✓	
3. جميع الجرائم الإلكترونية لها نفس المستوى من الخطورة والعواقب. **الجرائم الإلكترونية لها مستويات مختلفة من الخطورة والعواقب.**		✓
4. السرية والسلامة والمصادقة تُشكِّل مثلث أمن المعلومات. **يشكل مثلث أمن المعلومات: السرية، والسلامة، والتوافر.**		✓
5. الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز هو مؤسسة وطنية تهدف إلى تدريب المواهب المحلية في مجال الذكاء الاصطناعي.	✓	
6. تشير السلامة إلى التأكد من دقة البيانات وعدم التلاعب بها.	✓	
7. يُعدُّ التشفير والتحكم في الوصول وإخفاء البيانات من الطرائق المستخدَمة للحفاظ على سرية البيانات.	✓	
8. تضمن السرية أن البيانات دقيقة ولم يتم التلاعب بها. **تشير السرية إلى الحفاظ على القيود المُصرَّح بها للوصول إلى المعلومات، أي عدم السماح بالوصول للبيانات لمن لا يحق لهم الوصول إليها.**		✓
9. يُعدُّ رئيس إدارة الأمن السيبراني (CISO) مسؤولًا تنفيذيًا يشرف على برنامج الأمن السيبراني لمؤسسة معيَّنة.	✓	
10. يؤدّي رئيس إدارة الأمن السيبراني دورًا وظيفيًا في الأمن السيبراني.	✓	

يمكن تقديم إجابات إضافية من قبل الطلبة

2 اكتب وصفًا موجزًا لمجال الأمن السيبراني حسب ما يتطابق مع تعريف الهيئة الوطنية للأمن السيبراني.

الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.

3 صِفْ ما يمثله مثلث أمن المعلومات (CIA Triad) في مجال الأمن السيبراني.

مثلث أمن المعلومات (The CIA Triad) هو نموذج مُستخدَم على نطاق واسع لتصميم سياسات وممارسات الأمن السيبراني وتنفيذها، حيث يشير الاختصار CIA إلى السرية (Confidentiality - C) والسلامة (Integrity - I) والتوافر(Availability - A)، وهي الأهداف الرئيسة الثلاثة لحماية المعلومات والأنظمة من الوصول غير المصرَّح به أو التغيير أو الانقطاع.

يمكن تقديم إجابات إضافية من قبل الطلبة

4 وضِّح كيف تساعد السرية في حماية المعلومات الحساسة.

تشير السرية إلى الحفاظ على القيود المُصرَّح بها للوصول إلى المعلومات، أي عدم السماح بالوصول للبيانات لمن لا يحق لهم الوصول إليها، ويُمكن الحفاظ على السرية من خلال طرائق مختلفة مثل: التشفير، والتحكم في الوصول، وإخفاء البيانات. وتواجه السرية تهديدات محتملة مثل: هجمات التصيد الإلكتروني، حيث ينتحل المهاجِمون شخصيات كيانات شرعية لخداع الأفراد والحصول على معلومات حساسة.

5 اشرح سبب أهمية التوافر لضمان إمكانية وصول المُستخدِمين إلى الأنظمة والخدمات.

يشير التوافر إلى ضمان إمكانية الوصول إلى المعلومات عند الحاجة، ويُعدُّ ضروريًا لضمان إتاحة الأنظمة والخدمات للمُستخدِمين عند الحاجة، كما يُمكن أن يساعد تخزين نُسخ متعددة من البيانات، وعمل النسخ الاحتياطية، ووضع خُطط استعادة القدرة على العمل بعد الكوارث في ضمان التوافر.

يمكن تقديم إجابات إضافية من قبل الطلبة

6 حلِّل المبادرات المهنية الرئيسة لمجال الأمن السيبراني في المملكة العربية السعودية.

- التعليم والتدريب.
- استراتيجية الأمن السيبراني.
- الشراكات الصناعية.
- تطوير قطاع الأمن السيبراني.

تلميح: يمكنك توجيه الطلبة للرجوع إلى الصفحة رقم 15 من كتاب الطالب للحصول على الإجابة.

7 اشرح كيف أصبحت المملكة العربية السعودية واحدة من الدول الرائدة في تطوير أنظمة الأمن السيبراني وتشريعاته.

أصبحت المملكة العربية السعودية من أهم الدول الرائدة على مستوى العالم في مجال الأمن السيبراني، فهي تحتل المرتبة الثانية في المؤشر العالمي للأمن السيبراني (Global Cybersecurity Index - GCI) الذي يُعدُّ بمثابة مرجع دولي موثوق يقيس التزام الدول بالأمن السيبراني على المستوى العالمي، ويهتم بزيادة الوعي بأهمية الأمن السيبراني وأبعاده المختلفة.

مخاطر الأمن السيبراني وثغراته

وصف الدرس

الهدف العام من الدرس هو التعرف على مفهوم مخاطر الأمن السيبراني وثغراته، وأنواع الهجمات السيبرانية، بالإضافة إلى تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها.

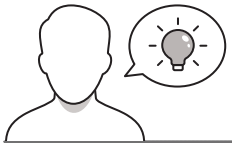
أهداف التعلُّم

- معرفة مفهوم مخاطر الأمن السيبراني وثغراته.
- تمييز أنواع الهجمات السيبرانية.
- تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها.

الدرس الثاني	
الوحدة الأولى: أساسيات الأمن السيبراني	عدد الحصص الدراسية
الدرس الثاني: مخاطر الأمن السيبراني وثغراته	3

نقاط مهمَّة

- قد يخلط بعض الطلبة بين أنواع **البرمجيات الضارة** (Malware) مثل: الفيروسات، والديدان، وأحصنة طروادة، وغيرها. وضّح لهم الفروق بينها، وقدّم الأمثلة على كل منها.
- قد لايدرك بعض الطلبة خطر الضغط على الروابط الاحتيالية المُرسلة عبر البريد الإلكتروني، وضّح لهم خطرها وأهمية التحقق من مصداقية الروابط قبل فتحها.



التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- مَن منكم قد تعرّض حاسوبه لهجمات ضارّة؟ وما السبب في نظركم؟
- هل تزعجكم البرمجيات الدعائية التي تظهر على المتصفحات أو التطبيقات؟ وكيف يمكنكم التخلص منها؟
- كيف يمكننا حماية كلمات المرور في أجهزتنا من الاختراق؟

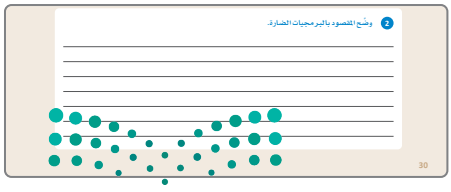
خطوات تنفيذ الدرس

> في البداية ناقش الطلبة حول مفاهيم الأمن السيبراني مثل: أصول الأمن السيبراني، وثغراته، ومخاطره، وهجمات الأمن السيبراني، ثم بيّن لهم المقصود بكلٍّ منها.

> وضّح لهم أنواع الجهات المسؤولة عن الهجمات السيبرانية، مستخدمًا الجدول (1.1)، وبيّن المهام المنوطة بكل منها.

> وضّح للطلبة الأنواع المختلفة للبرمجيات الضارة، وماهية كل منها، وخطرها، وكيفية الإصابة بها، وكيفية التخلص منها.

> وجّه الطلبة لحل التمرينات الثاني والثالث والرابع؛ للتحقق من فهمهم للبرمجيات الضارة وأنواعها المختلفة.



وزارة التعليم
Ministry of Education
2023 - 1445

- انتقل إلى شرح أنواع الهجمات السيبرانية، وبيّن لهم كيفية حدوث كل نوع، والأضرار التي يسببها.
- يمكنك بعدها تقسيم الطلبة لمجموعات متكافئة، واطلب من كل مجموعة اختيار مجموعة من أنواع الهجمات السيبرانية، وكتابة ملخص حول ماهيتها، واقتراح طرائق للحماية من الإصابة بها، وناقِش إجاباتهم، ثم قدّم التغذية الراجعة لهم.
- وجّه الطلبة لحل التمرينات الخامس والسادس والثامن والتاسع والعاشر؛ للتحقق من فهمهم لأنواع الهجمات السيبرانية وطرائق الوقاية منها.

أنواع الهجمات السيبرانية Types of Cyberattacks

بالإضافة إلى الهجمات التي تسببها البرمجيات الضارة، يُمكن استخدام العديد من أنواع الهجمات السيبرانية الأخرى لتعريض أنظمة الحاسب والشبكات والأجهزة للخطر. وفيما يلي بعض أكثر أنواع الهجمات السيبرانية شيوعًا:

هجمات الهندسة الاجتماعية Social Engineering Attacks

الهندسة الاجتماعية هي أحد أشكال التلاعب والخداع التي يستخدمها المهاجمون للحصول على معلومات حساسة من أجل الوصول غير المُصرّح به إلى الأنظمة المادية أو أنظمة الحاسب. حيث يحاول المهاجمون خداع المُستخدمين للكشف عن معلوماتهم الحساسة مثل: كلمات المرور، أو أرقام بطاقات الائتمان، أو غيرها من المعلومات الشخصية؛ وغالبًا ما تأتي هذه الهجمات على شكل رسائل بريد إلكتروني أو رسائل يبدو أنها من مصدر موثوق مثل: أحد البنوك أو أحد مواقع التواصل الاجتماعي الشهيرة. حيث تحتوي تلك الرسائل عادةً على رابط يوصل إلى موقع ويب مخادع أو مزيف صُمِّم ليبدو كموقع رسمي. حيث يُطلب من المُستخدم إدخال معلوماته. وفيما يلي بيان الأنواع الرئيسة لهجمات الهندسة الاجتماعية:

هجوم التصيد الإلكتروني (Phishing):
يتم خداع الضحايا من خلال الضغط على الروابط الاحتيالية المرسَلة عبر البريد الإلكتروني.

هجوم تصيد الرسائل القصيرة (Smishing):
يشابه هذا النوع التصيد الإلكتروني، إلا أنه يتم بإرسال رسالة نصية (SMS) تحتوي على نص جذاب على تطبيقات المراسلة. حيث يحتوي ذلك النص على رابط احتيالي.

هجوم التصيد الصوتي (Vishing):
يتصل مُرتكبو الجرائم السيبرانية بالضحايا المحتملين؛ في هذا النوع من الهجوم، مدّعين بأنهم شركة ما أو شخص معروف، وذلك بهدف الحصول على معلومات شخصية من الضحية.

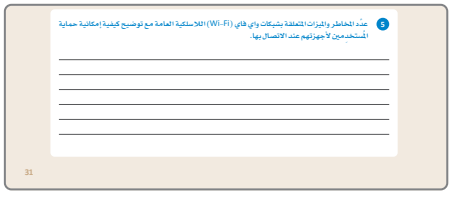
شكل 1.4: مثال على هجوم تصيد باستخدام الهندسة الاجتماعية

شكل 1.5: مثال على الروابط الاحتيالية

تثير رسائل البريد الإلكتروني التي تعتمد على التصيد الإلكتروني شعورًا بالقلق لدى المُستخدم من فقدان القدرة على الوصول إلى حساباته أو خدماته. وفيما يلي توضيح للخصائص الأكثر شيوعًا لتلك الرسائل المشبوهة التي قد تكون هجوم تصيد إلكتروني.

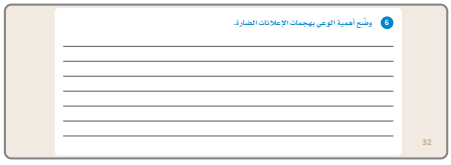
- تثير رسالة البريد الإلكتروني إن أن حسابك يُمثل بسبب مشكلة في الدفع.
- يحتوي البريد الإلكتروني على تحية عامة.
- يدعوك البريد الإلكتروني للضغط على رابط لتحديث تفاصيل الدفع الخاصة بك.

23



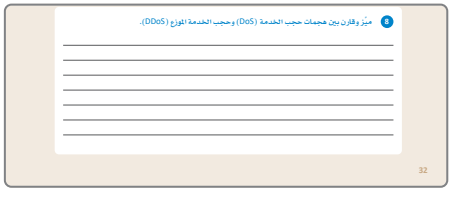
5 عدّد المخاطر والميزات المتعلقة بشبكات واي فاي (Wi-Fi) اللاسلكية العامة مع توضيح كيفية إمكانية حماية المُستخدمين لأجهزتهم عند الاتصال بها.

31



6 وضّح أهمية الوعي بهجمات الإعلانات الضارة.

32



8 ميّز وقارن بين هجمات حجب الخدمة (DoS) وحجب الخدمة الموزع (DDoS).

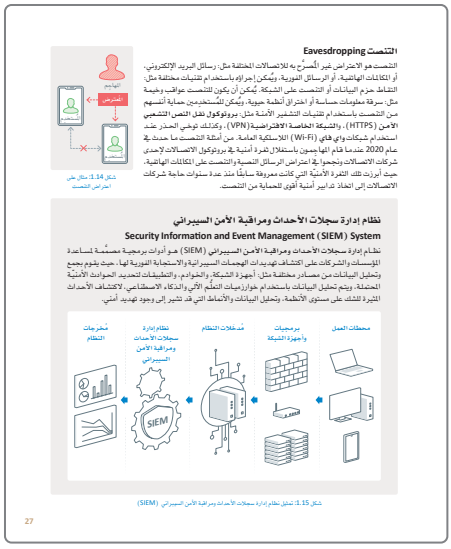
32

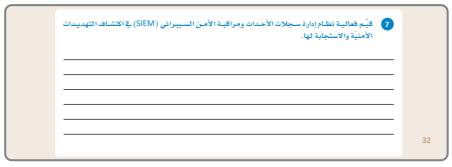
9 اذكر واشرح الخطوات التي يجب أن تتخذها أي مؤسسة للحماية من عمليات استغلال الثغرات الصفري.

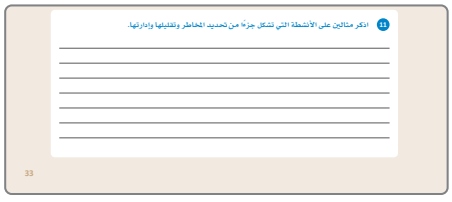
10 وضّح تأثير هجمات حقن النصوص البرمجية بلغة SQL على تطبيق الويب.

33

- اشرح للطلبة نظام إدارة **سجلات الأحداث ومراقبة الأمن السيبراني** (SIEM)، ثم وضّح لهم أهميتها في اكتشاف تهديدات الهجمات السيبرانية.
- وجّههم لحل التمرين السابع؛ للتحقق من فهمهم لنظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني.
- اشرح لهم كيفية تحديد مخاطر الأمن السيبراني، وكيفية تقليلها وإدارتها.
- وجّه الطلبة لحل التمرين الحادي عشر؛ للتأكد من فهمهم لكيفية تحديد مخاطر الأمن السيبراني.
- في الختام يمكنك توجيه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.







يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. الفيروس جزء من تعليمات برمجية يربط نفسه ببرنامج أو ملف آخر، ويتم تنفيذه عند تشغيل هذا البرنامج أو الملف.	✓	
2. تقوم برمجيات الفدية بتشفير ملفات المُستخدِم أو الجهاز، وتطالب بالدفع مقابل استعادتها.	✓	
3. حصان طروادة برنامج موثوق أو مفيد يُنفِّذ إجراءات مفيدة في الخلفية. يتنكر حصان طروادة كبرنامج موثوق أو مفيد.		✓
4. يُمكن أن تضيف المصادقة متعددة العوامل (MFA) طبقة حماية إضافية للحد من الهجمات التي تستهدف كلمات المرور.	✓	
5. برامج التجسس هي برمجيات ضارة تحمي خصوصية المُستخدِم وأمنه على الإنترنت. تنتهك برامجُ التجسس خصوصيةَ المُستخدِم والأمن عبر الإنترنت.		✓
6. هجمات التصيد الإلكتروني شكل من أشكال الهندسة الاجتماعية تحاول خداع المُستخدِمين للكشف عن معلومات حساسة.	✓	
7. تتضمن هجمات حجب الخدمة (DoS) التنسيق بين أجهزة متعددة لمهاجمة الشبكة في وقت واحد. يتم في هجوم حجب الخدمة (DoS) استخدام حاسب أو جهاز واحد لإغراق الشبكة.		✓
8. تستغل هجمات حقن النصوص البرمجية بلغة SQL الثغرات في قاعدة بيانات تطبيق الويب للوصول غير المُصرَّح به أو لإحداث تغييرات على البيانات.	✓	
9. تقوم هجمات البرمجة العابرة للمواقع (XSS) بحقن نصوص برمجية ضارة في موقع ويب لسرقة معلومات المُستخدِم أو التلاعب بالمحتوى المعروض.	✓	
10. لا تتعرض شبكات واي فاي (Wi-Fi) اللاسلكية العامة لهجمات التنصت. شبكات واي فاي (Wi-Fi) هي من أهداف هجمات التنصت.		✓

2 وضِّح المقصود بالبرمجيات الضارة.

البرمجيات الضارة: هي برامج صُممت لإلحاق الضرر بنظام الحاسب أو الشبكة، وتشمل الأنواع المختلفة من هذه البرامج الفيروسات، والديدان، وأحصنة طروادة، وبرمجيات الفدية، ويُمكن التمييز بين أنواع البرمجيات الضارة بناءً على آلية انتشارها والحمولة (Payload).

يمكن تقديم إجابات إضافية من قبل الطلبة

3 اشرح ماهية فيروس الحاسب وكيفية عمله.

الفيروس هو جزء من تعليمات برمجية ترتبط ببرنامج أو بملف آخر، ويتم تنفيذه عند تشغيل هذا البرنامج أو الملف، حيث يُمكن للفيروس إتلاف البيانات، أو حذفها، أو تعديل إعدادات النظام، أو الانتشار إلى ملفات أو أجهزة أخرى.

4 ميّز وقارن بين خصائص الفيروسات والديدان وأحصنة طروادة وبرمجيات الفدية.

- الفيروس هو جزء من تعليمات برمجية ترتبط ببرنامج أو بملف آخر، ويتم تنفيذه عند تشغيل هذا البرنامج أو الملف.
- حصان طروادة هو أحد أنواع البرمجيات الضارة التي تظهر كبرنامج موثوق أو مفيد، ولكنها في الحقيقة تُنفِّذ إجراءات ضارة على جهاز الحاسب في الخلفية دون علم مُستخدِم الجهاز.
- تشبه الديدان الفيروسات، ولكنها لا تحتاج إلى إرفاق نفسها ببرامج أو ملفات أخرى لمضاعفتها.
- برمجيات الفدية هي أحد أنواع البرمجيات الضارة التي تقوم بتأمين أو تشفير ملفات المُستخدِم أو الجهاز، وتطالب بالدفع مقابل استعادتها.

5 عدِّد المخاطر والميزات المتعلقة بشبكات واي فاي (Wi-Fi) اللاسلكية العامة مع توضيح كيفية إمكانية حماية المُستخدِمين لأجهزتهم عند الاتصال بها.

توفر شبكات واي فاي (Wi-Fi) العامة وصولًا سهلًا إلى الإنترنت، ولكنها تسبب للتعرض لخطر الهجمات مثل: هجمات الوسيط (Man-In-the-Middle)، والتنصت (Eavesdropping). يمكن للمُستخدِمين حماية أنفسهم باستخدام تقنيات التشفير مثل الشبكة الخاصة الافتراضية (VPN)، والوصول فقط إلى مواقع الويب والتطبيقات المؤمنة من خلال برتوكول أمن طبقة النقل(SSL).

يمكن تقديم إجابات إضافية من قبل الطلبة

6 وضِّح أهمية الوعي بهجمات الإعلانات الضارة.

قد يصعب اكتشاف الإعلانات الضارة، حيث تكون في الغالب جزءًا من الإعلانات الرسمية التي تقدمها الشركات المختلفة للمتصفحين، فبمجرد أن يضغط المُستخدِم على إعلان ضار، يتم تنزيل البرمجيات الضارة على حاسبه بحيث يُمكن استخدامها لسرقة معلوماته الحساسة أو تنفيذ هجمات أخرى.

7 قيِّم فعالية نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في اكتشاف التهديدات الأمنيّة والاستجابة لها.

نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني **(SIEM)** هو أدوات برمجية مصمَّمة لمساعدة المؤسسات والشركات على اكتشاف تهديدات الهجمات السيبرانية والاستجابة الفورية لها، حيث يقوم بجمع وتحليل البيانات من مصادر مختلفة مثل: أجهزة الشبكة، والخوادم، والتطبيقات لتحديد الحوادث الأمنيّة المحتملة، ويتم تحليل البيانات باستخدام خوارزميات التعلُّم الآلي والذكاء الاصطناعي، لاكتشاف الأحداث المثيرة للشك على مستوى الأنظمة، وتحليل البيانات والأنماط التي قد تشير إلى وجود تهديد أمني.

8 ميِّز وقارن بين هجمات حجب الخدمة (DoS) وحجب الخدمة الموزع (DDoS).

هجمات حجب الخدمة **(DoS)** وحجب الخدمة الموزع **(DDoS)** هي هجمات سيبرانية تعتمد على إغراق الشبكة أو الخادم بحركة بيانات ضخمة تجعل من الصعب أو حتى من المستحيل على المُستخدِمين الشرعيين الوصول إلى الخدمة، ويُمكن وصف هذا النوع من الهجمات بأنه هجوم على التوافر **(Availability)**، حيث يتم في هجوم حجب الخدمة **(DoS)** استخدام حاسب أو جهاز واحد لإغراق الشبكة، بينما يتم في هجوم حجب الخدمة الموزع **(DDoS)** استخدام أجهزة متعددة لمهاجمة الشبكة في وقت واحد.

يمكن تقديم إجابات إضافية من قبل الطلبة

9 اذكر واشرح الخطوات التي يجب أن تتخذها أي مؤسسة للحماية من عمليات استغلال الثغرات الصفري.

تكمن صعوبة الحماية من استغلال الثغرات الصفري في كونها غير معروفة لمُستخدِم البرنامج وكذلك لمن قاموا بإنشائه، وبالتالي لا يُمكن تصحيحها إلا حين يتم اكتشافها. يُمكن للمؤسسات حماية نفسها من هذه العمليات من خلال تنفيذ أفضل ممارسات الترميز الآمن، واستخدام أدوات الحماية التي يُمكنها اكتشاف السلوك المشبوه للبرامج وحظره.

10 وضِّح تأثير هجمات حقن النصوص البرمجية بلغة SQL على تطبيق الويب.

تستغل هجمات حقن النصوص البرمجية بلغة SQL الثغرات في قاعدة بيانات تطبيق الويب للوصول غير المُصرَّح به أو لإحداث تغييرات على البيانات، ويُمكن القيام بذلك من خلال إدخال تعليمات برمجية ضارة في حقول إدخال موقع الويب مثل: نماذج تسجيل الدخول، وذلك بهدف الوصول إلى قاعدة البيانات، كما يُمكن أن يكون لهذه الهجمات عواقب وخيمة مثل: سرقة البيانات الحساسة، أو تعديل سجلات قاعدة البيانات.

11 اذكر مثالين على الأنشطة التي تشكل جزءًا من تحديد المخاطر وتقليلها وإدارتها.

تحديد المخاطر

- تقييم التهديدات: يشمل تحديد مصادر التهديد المحتملة مثل: مُرتكبي الجرائم السيبرانية، أو التهديدات الداخلية، أو الكوارث الطبيعية، والتي يُمكن من خلالها استغلال الثغرات في أنظمة المؤسسة.
- تقييم الثغرات الأمنيّة: يشمل اكتشاف وتوثيق نقاط الضعف في الأصول الرقمية للمؤسسة باستخدام فحص الثغرات الأمنيّة، والقيام باختبارات الاختراق، وكذلك عمليات التقييم اليدوية الأخرى.

إدارة المخاطر

- تخطيط الاستجابة للحوادث: يشمل وضع خطة لاكتشاف الحوادث الأمنيّة والاستجابة لها، والتعافي منها؛ بهدف الحدّ من تأثيرها على المؤسسة في حال وقوعها.
- التحكم بالوصول: يشمل تنفيذ آليات للمصادقة والتفويض لتقييد الوصول إلى البيانات والأنظمة الحساسة وقصرها على المُستخدِمين المُصرَّح لهم بذلك.

تهديدات الأمن السيبراني وضوابطه

وصف الدرس

الهدف العام من الدرس هو التعرف على تهديدات الأمن السيبراني، وعلاقة الأمن السيبراني بالتحكم بالوصول، وتمييز أدواته، بالإضافة لتقييم وتحديد الثغرات الأمنيّة للأنظمة، وتمييز علاقة الأمن السيبراني بالقرصنة الأخلاقية.

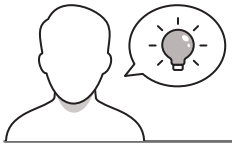
أهداف التعلُّم

- معرفة تهديدات الأمن السيبراني.
- معرفة علاقة الأمن السيبراني بالتحكم بالوصول.
- تمييز أدوات التحكم بالوصول.
- تقييم وتحديد الثغرات الأمنيّة للأنظمة.
- تمييز علاقة الأمن السيبراني بالقرصنة الأخلاقية.

الدرس الثالث	
الوحدة الأولى: أساسيات الأمن السيبراني	عدد الحصص الدراسية
الدرس الثالث: تهديدات الأمن السيبراني وضوابطه	3

نقاط مهمَّة

- قد يخلط بعض الطلبة بين تهديدات الأمن السيبراني، وضّح كل واحدة على حِدة، وقدّم مثالًا لكل منها من الواقع لتسهيل فهمهم لها.
- قد تخفى على بعض الطلبة طرائق المصادقة متعددة العوامل، وضّح لهم أبرزها، وبيّن كيف يمكنهم استخدامها لحماية أجهزتهم من خلالها.

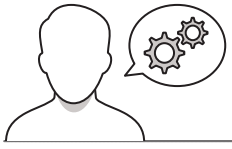


التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- ماذا نقصد بانتحال الشخصية؟
- هل تستخدمون المصادقة متعددة العوامل في أجهزتكم؟ مَن يقدِّم مثالًا عليها؟
- هل يمكن أن تكون هناك قرصنة أخلاقية؟ وكيف ذلك؟



خطوات تنفيذ الدرس

> في البداية ناقِش الطلبة حول المقصود بتهديدات الأمن السيبراني، وبيّن لهم الفرق بين أنواعها من خلال الأمثلة الواقعية.

> ناقشهم حول مفهوم انتحال الشخصية، واطلب منهم تقديم الأمثلة عليه من بيئتهم المحيطة من خلال التجارب التي سمعوا بها.

> وجّه الطلبة لحل التمرينين الثاني والثالث؛ للتحقق من فهمهم لخطر تهديدات الأمن السيبراني.

> انتقل بعد ذلك إلى شرح علاقة الأمن السيبراني بالتحكم بالوصول، وبيّن لهم أنواعه المختلفة، ومثّل لكل نوع.


الدرس الثالث
تهديدات الأمن السيبراني وضوابطه

تهديدات الأمن السيبراني Cybersecurity Threats

أصبحت تهديدات الأمن السيبراني تُشكّل خطرًا دائمًا في عالمنا الذي يعتمد على التقنية بشكل متزايد. ومع ازدياد الأنشطة التي تتم عبر الإنترنت، أصبح الوصول إلى البيانات الشخصية أكثر سهولة. وتتعرض فيها المخاطر الرئيسة لتحديات الأمن السيبراني أمرًا محتمًا، ومن أمثلة تلك المخاطر: تهديدات البيانات، وانتحال الشخصية، والتتبُّع عبر الإنترنت.

تهديدات البيانات Data Threats

تُعدّ حماية البيانات أمرًا بالغ الأهمية في ظل تخزين المزيد من المعلومات الشخصية والحساسة رقميًا، حيث يجب على المؤسسات التعامل مع البيانات الشخصية بشكل آمن ومسؤول، وحمايتها من الوصول غير المشروع، أو التغيير أو الكشف غير المُصرَّح به. وتشمل مخاوف حماية البيانات الرئيسة ما يلي:

خروقات البيانات (Data Breaches):	الاحتفاظ بالبيانات (Data Retention):	سيادة البيانات (Data Sovereignty):
الوصول غير المُصرَّح به إلى البيانات الشخصية، أو الكشف عنها، وهذا غالبًا بسبب ضعف التدابير الأمنية أو خطأ بشري.	يُمكن أن تثير المدة والطريقة التي يتم بها تخزين البيانات الشخصية المخاوف خاصةً إذا كانت البيانات المخزّنة غير محمية بشكل كافٍ.	الأثار القانونية لتخزين البيانات في بلدان مختلفة مما قد يتسبب في تطبيق قوانين وأنظمة خصوصية مختلفة على هذه البيانات وفقًا لقوانين كل دولة.

انتحال الشخصية Identity Theft

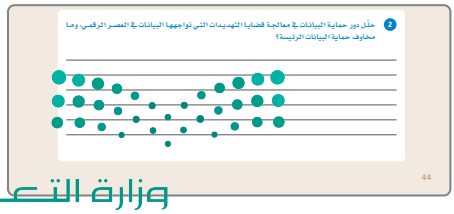
يحدث انتحال الشخصية من خلال سرقة المعلومات الشخصية لفرد ما واستخدامها بطريقة احتيالية؛ لتحقيق مكاسب مالية غالبًا، وأتاح العصر الرقمي لمرتكبي الجرائم الوصول إلى البيانات الشخصية واستغلالها، مما زاد من عمليات انتحال الشخصية. ومن الأمثلة عليها:

انتحال الهوية (Spoofing):	هجوم التصيد المستهدف (Spear-Phishing):
انتحال الهوية هو تكرار المهاجم كمُستخدم شرعي للنظام من أجل الوصول إلى المعلومات.	يُوجّه هجوم التصيد المستهدف إلى الأفراد أو المؤسسات برسائل مخصصة بهدف الحصول على معلوماتهم الحساسة والشخصية، حيث يستخدم المهاجم المعلومات الشخصية المضحية لجعل الرسالة تبدو من مصدر رسمي.

التتبُّع الإلكتروني Online Tracking

يخضع الكثير من الأشخاص للتتبُّع والمراقبة عند القيام بالأنشطة المختلفة عبر الإنترنت، مما يثير مخاوف بشأن الخصوصية والمراقبة. وتوجد بعض الممارسات المشروعة أو الإيجابية (غير المشروعة) للتتبُّع الإلكتروني مثل:

34


2 حلّل دور حماية البيانات في معالجة قضايا التهديدات التي تواجهها البيانات في العصر الرقمي وما مخاوف حماية البيانات الرئيسة؟

44


3 قيّم استخدام ملفات تعريف الارتباط في التتبُّع عبر الإنترنت وكيف يُمكنها تحسين تجربة المُستخدم أو إثارة مخاوفه بشأن الخصوصية؟

45

- واصل الشرح باستعراض أدوات التحكم بالوصول للأمن السيبراني، واشرح أنواعه، ثم اعرض لهم المثال على **الدليل النشط** (Active Directory) من خلال الشكل (1.17).
- اشرح لهم طرائق مهاجمة **إدارة الهوية والوصول** (Identity and Access Management – IAM)، وقدّم الأمثلة عليها.
- يمكنك بعد ذلك توجيه الطلبة لحل التمرينين الرابع والخامس؛ للتأكد من فهمهم لأهمية التحكم بالوصول في الأمن السيبراني.
- انتقل بعدها لشرح تقييم وتحديد الثغرات الأمنيّة للأنظمة، وبيّن لهم الجوانب التي يشملها **تقييم الثغرات الأمنيّة** (Vulnerability Assessment – VA)، والجوانب الرئيسة **لاختبار الاختراق** (Penetration Testing – PT).

شكل 1.17: هيكلة الدليل النشط

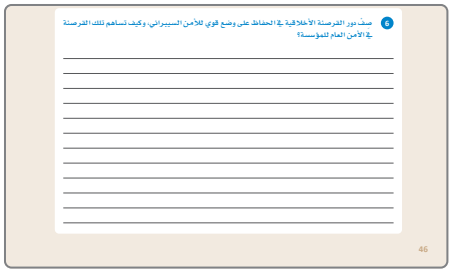
- استمر في الشرح بتوضيح مفهوم القرصنة الأخلاقية، وعلاقتها بالأمن السيبراني، وبيّن لهم الجوانب الحاسمة للحفاظ على التوازن والموضوعية في القرصنة الأخلاقية.
- يمكنك بعدها تقسيم الطلبة لمجموعات متكافئة، واطلب من كل مجموعة مناقشة الأنشطة الرئيسة التي يؤديها مختصو الأمن السيبراني بالاستعانة بالجدول (1.5)، وناقِش إجاباتهم، ثم قدّم التغذية الراجعة لهم.


جدول 1.5: الأنشطة الرئيسة التي يؤديها متخصصو الأمن السيبراني

النشاط	الوصف
اختبار الاختراق	تقييد اختبارات الاختراق لمحاكاة الهجمات على أنظمة المؤسسة أو شبكاتها أو تطبيقاتها، وتساعد هذا في تحديد الثغرات الأمنية القابلة للاستغلال وتقييم فعالية الضوابط الأمنيّة الحالية.
تقييمات الثغرات الأمنيّة	إجراء تقييمات للثغرات الأمنيّة عن طريق فحص الأنظمة والتطبيقات بحثًا عن الثغرات الأمنيّة أو الإعدادات الخاطئة أو نقاط الضعف المعروفة، ثم يتم تقديم تقرير مُفصّل عن النتائج التي تم التوصل إليها وترتيب أولوية الثغرات الأمنيّة حسب خطورتها من أجل علاجها.
تدقيقات الأمن	إجراء عمليات تدقيق أمنية شاملة للبنية التحتية للمؤسسة وسياساتها وإجراءاتها لتقييم وضعها الأمني العام وتحديد مجالات التحسين والتطوير.
تقييمات الهندسة الاجتماعية	إجراء تقييمات الهندسة الاجتماعية لتقييم قابلية المؤسسة للتعرض للهجمات على العنصر البشري مثل: التصيد الإلكتروني، أو الخداع، أو الاختراق الأمني. كما يُمكن أيضًا تقديم التوصيات لتحسين الوعي والتدريب الأمني للموظفين.
تقييمات الشبكة اللاسلكية	تقييم أمن الشبكات اللاسلكية للمؤسسة، بما في ذلك شبكات الواي فاي (Wi-Fi) والبلوتوث (Bluetooth) لتحديد الثغرات الأمنيّة، أو التشفير الضعيف، أو الإعدادات الخاطئة التي قد يستغلها المهاجمون.
اختبار تطبيق الويب	اختبار تطبيقات الويب بحثًا عن أي ثغرات أمنية محتملة مثل: حقن النصوص البرمجية بلغة SQL، أو الهجوم البرمجي العابر للمواقع، أو تجاوز عمليات المصادقة، مما يساعد المؤسسات على تأمين خدماتها عبر الإنترنت وحماية بياناتها الحساسة.
ممارسات فريق الأمن الأحمر	المشاركة في أنشطة فريق الأمن الأحمر، والتصرف كمها جمي أنظمة ضمن سيناريو محاكاة يختبر قدرة استجابة المؤسسة للحوادث، واستعداداتها الأمنيّة، ومرونتها الشاملة.
مراجعة التعليمات البرمجية الآمنة	مراجعة التعليمات البرمجية الخاصة بالمؤسسة بحثًا عن الثغرات الأمنيّة، أو نقاط الضعف المحتملة، ثم تقديم التوصيات لتحسين أمن التعليمات البرمجية وتقليل مخاطر الاستغلال.
التدريب والتوعية الأمنيّة	[illegible] على تطوير وتقديم برامج التدريب الأمني [illegible] والمعرفة بتقنيات [illegible] أفضل ممارسات الأمن [illegible] وتحسين سلوكيات الموظفين [illegible]

43

- بنفس المجموعات السابقة، وجّه الطلبة لحل التمرينات السادس والسابع والثامن؛ بهدف التحقق من فهمهم لدور القرصنة الأخلاقية في الأمن السيبراني.
- في الختام اطلب منهم حل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.



وزارة التعليم
Ministry of Education
2023 - 1445

يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. هجمات التصيد المستهدف هي هجمات موزعة ذات مصادر متعددة تستهدف مجموعة كبيرة من الأشخاص. هجمات التصيد المستهدف هي هجمات أكثر تركيزًا وشخصية.	○	✓
2. ملفات تعريف الارتباط هي ملفات نصية صغيرة يتم وضعها على جهاز المُستخدِم بواسطة مواقع الويب لتَتبُّع نشاط التصفح.	✓	○
3. يتم استخدام تَتبُّع السلوك حصريًا للأغراض الأمنيّة وليس للإعلانات المستهدفة. تعدُّ الإعلانات المستهدفة أحد الاستخدامات الرئيسة للتَتبُّع السلوك.	○	✓
4. لا يُعدُّ التحكم بالوصول هامًا لحماية أنظمة المعلومات وخصوصية البيانات من الوصول غير المُصرَّح به والتعديل. يُعدُّ التحكم بالوصول أحد تدابير الحماية الأساسية.	○	✓
5. ينص مبدأ الحد الأدنى من الصلاحيات والامتيازات على أنه يجب منح المُستخدِمين الحد الأقصى من مستوى الوصول اللازم لأداء أدوارهم الوظيفية. ينص مبدأ الحد الأدنى أنه يجب منحهم الحد الأدنى من مستوى الوصول.	○	✓
6. تُعدُّ نماذج التحكم بالوصول مثل التحكم في الوصول بناءً على السمات (ABAC) والتحكم في الوصول بناءً على الدور (RBAC) مسؤولة عن فرض سياسات الأمن وإدارة وصول المُستخدِم داخل المؤسسة.	✓	○
7. تتماثل القرصنة الأخلاقية مع القرصنة الخبيثة من حيث النوايا والسماح. الهدف النهائي للقرصنة الأخلاقية هو تحسين الوضع الأمني للأنظمة.	○	✓
8. يجب أن يعمل القراصنة الأخلاقيون دائمًا بإذن صريح من المؤسسة التي يختبرونها.	✓	○
9. الإفصاح والمعالجة من الجوانب الأساسية للقرصنة الأخلاقية للحفاظ على الثقة ومعالجة القضايا الأمنيّة بشكل فعَّال.	✓	○
10. يقوم فريق قراصنة القبعات البيضاء بعمل تقييمات الهندسة الاجتماعية لمعرفة مدى قدرة المؤسسة الأمنيّة على مواجهة الهجمات على العنصر البشري.	✓	○

يمكن تقديم إجابات إضافية من قبل الطلبة

2 حلِّل دور حماية البيانات في معالجة قضايا التهديدات التي تواجهها البيانات في العصر الرقمي، وما مخاوف حماية البيانات الرئيسة؟

تُعدُّ حماية البيانات أمرًا بالغ الأهمية في ظل تخزين المزيد من المعلومات الشخصية والحساسة رقميًا، حيث يجب على المؤسسات التعامل مع البيانات الشخصية بشكل آمن ومسؤول، وحمايتها من الوصول غير المشروع، أو التغيير أو الكشف غير المُصرَّح به، وتشمل مخاوف حماية البيانات الرئيسة ما يلي:

- خروقات البيانات: الوصول غير المُصرَّح به إلى البيانات الشخصية، أو الكشف عنها، وهذا غالبًا بسبب ضعف التدابير الأمنيّة أو خطأ بشري.

- الاحتفاظ بالبيانات: يُمكن أن تثير المدة والطريقة التي يتم بها تخزين البيانات الشخصية المخاوف خاصةً إذا كانت البيانات المخزَّنة غير محمية بشكل كافٍ.

- سيادة البيانات: الآثار القانونية لتخزين البيانات في بلدان مختلفة مما قد يتسبب في تطبيق قوانين وأنظمة خصوصية مختلفة على هذه البيانات وفقًا لقوانين كل دولة.

3 قيِّم استخدام ملفات تعريف الارتباط في التَتبُّع عبر الإنترنت، وكيف يُمكنها تحسين تجربة المُستخدِم أو إثارة مخاوفه بشأن الخصوصية؟

ملفات تعريف الارتباط: هي ملفات نصية صغيرة يتم وضعها على جهاز المُستخدم بواسطة مواقع الويب لتَتبُّع نشاط التصفح والتفضيلات لأغراض مشروعة، مثل تخصيص المحتوى، ولكن يُمكن أيضًا استخدامها لجمع البيانات دون موافقة المُستخدِم.

4 حلِّل أهمية عدم الإنكار في التحكم بالوصول والأمن السيبراني.

يُعدُّ عدم الإنكار جانبًا مهمًا من جوانب التحكم بالوصول والأمن السيبراني، حيث يضمن عدم تمكن المُستخدمين من إنكار صحة أفعالهم أو مُعامَلاتهم داخل النظام، ويحمل هذا الأمر أهمية خاصة في الحالات التي يجب فيها الحفاظ على سلامة البيانات أو صحة المُعامَلات مثل: الخدمات المالية، والرعاية الصحية، والمُعامَلات القانونية، كما يُمكن أن يساعد تنفيذ آليات عدم الإنكار في منع النزاعات والاحتيال والأنشطة غير المُصرَّح بها من خلال تقديم أدلة دامغة على إجراءات المُستخدِمين.

يمكن تقديم إجابات إضافية من قبل الطلبة

5 قيِّم مبدأ الحد الأدنى من الصلاحيات والامتيازات وتأثيره على التحكم بالوصول، وكيف يؤدي الالتزام بهذا المبدأ إلى تقليل المخاطر الأمنيّة داخل المؤسسة؟

من المهم أن تلتزم أنظمة التحكم بالوصول بمبدأ الحد الأدنى من الصلاحيات والامتيازات الذي ينص على أنه يجب منح المُستخدمين الحد الأدنى من مستوى الوصول اللازم لأداء أدوارهم الوظيفية، ويَحدُّ هذا من إمكانية الوصول غير المُصرَّح به، أو إساءة استخدام البيانات الحساسة ويسهم في تقليل الضرر المحتمل الناجم عن اختراق حسابات المُستخدِمين أو التهديدات الداخلية.

6 صِفْ دور القرصنة الأخلاقية في الحفاظ على وضع قوي للأمن السيبراني، وكيف تساهم تلك القرصنة في الأمن العام للمؤسسة؟

يُطلق لقب القراصنة الأخلاقيون أو القراصنة ذوي القبعات البيضاء على القراصنة الذين يستخدمون التقنيات والأدوات لتحديد الثغرات الأمنيّة ونقاط ضعف أنظمة المؤسسة، أو شبكاتها، أو تطبيقاتها. يتمثل الاختلاف الأساسي بين القرصنة الأخلاقية والقرصنة الخبيثة في الإجراءات المُستخدَمة والأذونات الممنوحة من المؤسسة المستهدَفة، حيث يعمل القراصنة الأخلاقيون ضمن الحدود القانونية والأخلاقية لمساعدة المؤسسات على تحسين وضعها الأمني، بينما يهدف القراصنة الخبثاء إلى استغلال الثغرات الأمنيّة لأغراض خبيثة أو لتحقيق مكاسب شخصية.

يمكن تقديم إجابات إضافية من قبل الطلبة

7 وضِّح دور الاحترافية والمسؤولية في القرصنة الأخلاقية.

الالتزام بقواعد السلوك الصارمة وإثبات الاحترافية، بحيث يتحمل القراصنة الأخلاقيون مسؤولية أفعالهم ويحرصون على عدم التسبب في أي ضرر للأنظمة التي يختبرونها.

8 قيِّم دور القراصنة ذوي القبعات البيضاء في إجراء عمليات تدقيق الأمن وممارسات فريق الأمن الأحمر.

- عمليات تدقيق الأمن: إجراء عمليات تدقيق أمنية شاملة للبنية التحتية للمؤسسة وسياساتها وإجراءاتها لتقييم وضعها الأمني العام وتحديد مجالات التحسين والتطوير.
- ممارسات فريق الأمن الأحمر: المشاركة في أنشطة فريق الأمن الأحمر، والتصرف كمهاجمي أنظمة ضمن سيناريو محاكاة يختبر قدرة استجابة المؤسسة للحوادث، واستعداداتها الأمنيّة، ومرونتها الشاملة.

المشروع

أهداف المشروع:

- استعراض التهديدات من البرمجيات الضارة والهجمات السيبرانية المتقدمة.
- تحديد مهام إدارة المخاطر التي تساعد على التقليل من تأثيرها.
- تحليل التهديدات التي تواجهها الشركات.
- تحديد الخطوات المقترحة لتأمين أنظمة معلومات الخاصة بالشركات.

- قسّم الطلبة لمجموعات متكافئة، واطلب منهم تخطيط المشروع قبل البدء فيه.
- وجّههم للرجوع للمفاهيم النظرية والخطوات العملية في الوحدة عند الحاجة.
- ضع معايير مناسبة لتقييم أعمال الطلبة في المشروع، وتأكّد من فهم لمتطلبات المشروع.
- يمكنك الاسترشاد بمعايير تقييم المشاريع الواردة في الدليل العام.
- قيّمهم وَفْقَ معايير التقييم، وقدّم لهم التغذية الراجعة للوصول لأفضل نتيجة.
- أخيرًا، حدِّد موعد تسليم المشروع ومناقشة أعمال المجموعات.

سُلّم التقدير

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
المعرفة: تعريف البرمجيات الضارة، وعرض أمثلة عليها، وشرح عواقب الهجمات الضارة على نظام معلومات الشركة	عرّفَ البرمجيات الضارة، ولم يذكر أمثلة عليها، ولم يشرح عواقب الهجمات الضارة.	عرّفَ البرمجيات الضارة، وعرَضَ مثالًا واحدًا عليها، ولم يشرح عواقب الهجمات الضارة.	عرّفَ البرمجيات الضارة، وعرَضَ أكثر من مثال عليها، ولم يشرح عواقب الهجمات الضارة.	عرّفَ البرمجيات الضارة، وعرَضَ أكثر من مثال عليها، وشَرحَ عواقب الهجمات الضارة.
المعرفة: تحديد المخاطر، وتقييمها، ووصف الاستراتيجيات المستخدَمة لتقليل المخاطر المرتبطة بالبرمجيات الضارة والهجمات السيبرانية	لم يحدِّد المخاطر، ولم يقيّمها، ولم يصف الاستراتيجيات المستخدَمة لتقليل المخاطر المرتبطة بالبرمجيات الضارة والهجمات السيبرانية.	حدَّدَ المخاطر، ولم يقيّمها، ولم يصف الاستراتيجيات المستخدَمة لتقليل المخاطر المرتبطة بالبرمجيات الضارة والهجمات السيبرانية.	حدَّدَ المخاطر، وقيّمها، ولم يصف الاستراتيجيات المستخدَمة لتقليل المخاطر المرتبطة بالبرمجيات الضارة والهجمات السيبرانية.	حدَّدَ المخاطر، وقيّمها، ووصفَ الاستراتيجيات المستخدَمة لتقليل المخاطر المرتبطة بالبرمجيات الضارة والهجمات السيبرانية.
المهارة: عرض دراسات حالة لمؤسسات تمكّنت بشكل فعّال من إدارة المخاطر التي تشكلها البرمجيات الضارة والهجمات السيبرانية المتقدمة	لم يعرض دراسات حالة لمؤسسات تمكّنت بشكل فعّال من إدارة المخاطر التي تشكلها البرمجيات الضارة والهجمات السيبرانية المتقدمة.	عرضَ دراسات حالة واحدة لمؤسسات تمكّنت بشكل فعّال من إدارة المخاطر التي تشكلها البرمجيات الضارة والهجمات السيبرانية المتقدمة.	عرضَ دراستي حالة لمؤسسات تمكّنت بشكل فعّال من إدارة المخاطر التي تشكلها البرمجيات الضارة والهجمات السيبرانية المتقدمة.	عرضَ ثلاث دراسات حالة لمؤسسات تمكّنت بشكل فعّال من إدارة المخاطر التي تشكلها البرمجيات الضارة والهجمات السيبرانية المتقدمة.
المهارة: إنشاء عرض تقديمي باستخدام باوربوينت يشتمل على أهمية استراتيجيات الأمن السيبراني، بالإضافة للملاحظات أعلاه	أنشَأ عرضًا تقديميًّا يتضمن فقرة حول أهمية استراتيجيات الأمن السيبراني.	أنشَأ عرضًا تقديميًّا يتضمن فقرتين حول أهمية استراتيجيات الأمن السيبراني.	أنشَأ عرضًا تقديميًّا يتضمن ثلاث فقرات حول أهمية استراتيجيات الأمن السيبراني.	أنشَأ عرضًا تقديميًّا يتضمن أربع فقرات فأكثر حول أهمية استراتيجيات الأمن السيبراني.

تلميح: محكات المعرفة والمهارات تعتبر أساسية لاستيفاء أهداف المشروع بينما يمكن للمعلّم استخدام محكات (التفكير الناقد / الإبداع / العمل مع الآخرين / العرض) حسب ما يراه مناسب.

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
التفكير الناقد	لا يظهر فهمًا للمشكلة أو أهداف المهمة، وينظر لها بشكل سطحي، ويقبل المعلومات من غير تقييم لمصداقيتها.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد بعض الجوانب لما يجب معرفته وطرح الأسئلة. يحاول دمج المعلومات التي تم جمعها. يدرك أهمية مصداقية المعلومات لكن لا يتخذ إجراءات للتأكد من ذلك.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد بعض الجوانب لما يجب معرفته وطرح الأسئلة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها. يقيم الحجج من خلال تقييم الأدلة الداعمة لها.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد ما يجب معرفته، وطرح الأسئلة حسب الحاجة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها ويقيم مصداقيتها، ويميز بين الحقيقة والرأي. يقيم الحجج من خلال تقييم الأدلة الداعمة لها. ويبرر سبب القبول أو الرفض وفق معايير محددة وواضحة.
الإبداع	يولد عددًا محدودًا من الأفكار التي لا ترتبط بالمشكلة أو أهداف المهمة. المنتج نسخة لأمثلة أو إجابات نموذجية سابقة.	يولد عددًا محدودًا من الأفكار التي قد ترتبط بالمشكلة أو أهداف المهمة. المنتج نسخة لأمثلة أو إجابات نموذجية سابقة أو يتضمن توظيف أكثر من طريقة معروفة مسبقًا.	يولد عددًا محدودًا من الأفكار ذات الصلة المباشرة بالمشكلة أو أهداف المهمة. يتضمن المنتج بعض الجوانب المبتكرة، ويتصف بالفائدة العملية.	يولد عددًا من الأفكار ذات الصلة المباشرة بالمشكلة أو أهداف المهمة، ويستخدمها لتطوير حل للمشكلة أو تحقيق أهداف المهمة. يتصف المنتج بالأصالة والابتكار والفائدة العملية.
العمل مع الآخرين	غير مستعد للعمل والتعاون مع الآخرين، لا يشارك في حل المشكلات أو طرح الأسئلة أو المناقشات.	يقوم ببعض المهام في المشروع ويتعاون مع الفريق، ولكن قد لا يساهم بنشاط في حل المشكلات أو طرح الأسئلة أو المناقشات.	يقوم بأداء مهامه في المشروع، يتعاون مع الفريق ويساهم في حل المشكلات وطرح الأسئلة والمناقشات، ويعطي ملاحظات لمساعدة الفريق.	يقوم بأداء مهامه في المشروع ويكملها في الوقت المحدد، يتعاون مع الفريق ويساهم في حل المشكلات وطرح الأسئلة والمناقشات بناءً على الأدلة، ويعطي ملاحظات بناءة لمساعدة الفريق وتحسين العمل.

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
العرض	لا يفي بمتطلبات ما يجب تضمينه في العرض، لا يقدم معلومات واضحة، يستخدم أسلوبًا غير مناسب لأهداف المهمة والجمهور.	يلبي بعض المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة)، يقدم بعض المعلومات الواضحة، ويستخدم أسلوبًا مناسبًا نوعًا ما لأهداف المهمة والجمهور.	يفي بمعظم المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة واضحة)، يقدم المعلومات بوضوح، ويستخدم أسلوبًا مناسبًا لأهداف المهمة والجمهور.	يفي بجميع المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة واضحة ومثيرة للاهتمام، ينظم الوقت بشكل جيد)، يقدم جميع المعلومات بوضوح ودقة وفق تسلسل منطقي، ويستخدم أسلوبًا مناسبًا لأهداف المهمة والجمهور.

الوحدة الثانية

الحماية والاستجابة في الأمن السيبراني

وصف الوحدة

عزيزي المعلّم

الغرض العام من الوحدة هو أن يحدِّد الطلبة التهديدات والثغرات الأمنيّة التي تؤثر على أمن العتاد ونظام التشغيل والبرمجيات، ويحلّلوا تقنيات تصميم النظام الآمن، ويطبقوا إجراءات الأمن الأساسية لحماية الأجهزة والبيانات في ويندوز، ويصفوا تأثير هياكل الشبكات وتقنيات الويب على أنظمة الأمن السيبراني، ويوضحوا بروتوكولات أمن الشبكة وتقنياتها، ويحلّلوا حركة بيانات الشبكة باستخدام برنامج **وايرشارك** (Wireshark)، بالإضافة إلى استخدام خدمة الشبكة الافتراضية الخاصة في ويندوز، وتحليل كيفية استخدام التحليل الجنائي الرقمي والاستجابة للحوادث في حماية الأنظمة الرقمية.

أهداف التعلُّم

- تحديد التهديدات والثغرات الأمنيّة التي تؤثر على أمن العتاد ونظام التشغيل والبرمجيات.
- تحليل تقنيات تصميم النظام الآمن.
- تطبيق إجراءات الأمن الأساسية لحماية الأجهزة والبيانات في ويندوز.
- وصف تأثير هياكل الشبكات وتقنيات الويب على أنظمة الأمن السيبراني.
- توضيح بروتوكولات أمن الشبكة وتقنياتها.
- تحليل حركة بيانات الشبكة باستخدام برنامج واير شارك (Wireshark).
- استخدام خدمة الشبكة الافتراضية الخاصة في ويندوز (Windows VPN).
- تحليل كيفية استخدام التحليل الجنائي الرقمي والاستجابة للحوادث في حماية الأنظمة الرقمية

الدروس	
الوحدة الثانية : الحماية والاستجابة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: أمن العتاد والبرمجيات ونظام التشغيل	4
الدرس الثاني: أمن الشبكات والويب	4
الدرس الثالث: التحليل الجنائي الرقمي والاستجابة للحوادث	4
المشروع	3
إجمالي عدد حصص الوحدة الثانية	15

المصادر والملفات والأدوات والأجهزة المطلوبة

المصادر

كتاب الأمن السيبراني

التعليم الثانوي – نظام المسارات

السنة الثالثة

الملفات الرقمية

يُمكنك الوصول للحلول أو الملفات النهائية للتمرينات التي يمكن استخدامها على منصة "عين" الإثرائية، وهي:

- مجلد G12.CYB.S3.U2

الأدوات والأجهزة

- **برنامج واير شارك** (Wireshark)
- **جدار حماية ويندوز ديفندر** (Windows Defender Firewall)
- **متصفح دي بي إس كيو لايت** (DB Browser for SQLite)

أمن العتاد والبرمجيات ونظام التشغيل

وصف الدرس

الهدف العام من الدرس هو التعرف على أمن العتاد والبرمجيات ونظام التشغيل، وتقنيات تصميم النظام الآمن، وتنشيط جدار حماية ويندوز، وكيفية السماح لتطبيقات الحاسب بالوصول إلى الإنترنت، بالإضافة لتعديل أذونات الملفات والمجلدات على الحاسب.

أهداف التعلُّم

- معرفة أمن العتاد والبرمجيات ونظام التشغيل.
- معرفة تقنيات تصميم النظام الآمن.
- تنشيط جدار حماية ويندوز.
- السماح لتطبيقات الحاسب بالوصول إلى الإنترنت.
- تعديل أذونات الملفات والمجلدات على الحاسب.

الدرس الأول	
الوحدة الثانية: الحماية والاستجابة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: أمن العتاد والبرمجيات ونظام التشغيل	4

نقاط مهمَّة

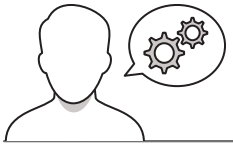
- قد يخفى على بعض الطلبة ضرورة مصادقة المُستخدِم لحماية أنظمة التشغيل، بيّن لهم أهمية استخدام اسم مُستخدِم فريد وكلمة مرور قوية ومعقدة لحماية حسابات المُستخدِمين من التهديدات الشائعة.
- قد لا يدرك بعض الطلبة أهمية وجود سعة كافية للبيانات في أنظمة البرمجيات، بيّن لهم أن إدخال كميات كبيرة من البيانات أكبر من السعة المخصصة يمكن أن تتسبب بتعطل النظام، مما قد يسمح بتشغيل التعليمات البرمجية الضارة.

التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- ماذا نقصد بالعتاد في الحاسب؟ وهل يمكن أن يتعرض لهجمات وتهديدات؟
- هل سبق لأحدكم أن استخدم برنامج مكافحة فيروسات؟ ولماذا؟
- ما جدار حماية ويندوز؟ وما أهميته؟



خطوات تنفيذ الدرس

> في البداية ناقِش الطلبة حول أهمية أمن العتاد والبرمجيات وأنظمة التشغيل في الأمن السيبراني.

> اشرح لهم أهم التهديدات التي يمكن أن تصيب عتاد الحاسب، وبيّن ممارسات الأمان لحماية أنظمة العتاد.

> انتقل إلى شرح أمن نظام التشغيل، ووضّح لهم التهديدات التي يتعرض لها، ثم بيّن أهم ممارسات الأمان للحماية من تلك التهديدات.

> بنفس الطريقة السابقة، اشرح لهم أيضًا أهم التهديدات التي يمكن أن تتعرض لها أنظمة البرمجيات في الحاسب، وأهم ممارسات الأمان للحماية من تلك التهديدات.

> يمكنك بعدها تقسيم الطلبة لمجموعات متكافئة، واطلب من كل مجموعة تلخيص أبرز التهديدات التي يمكن أن تصيب عتاد الحاسب، وأنظمة التشغيل، والبرمجيات، ثم كتابة أهم ممارسات الأمان لحماية نظام العتاد. وناقِش إجاباتهم، ثم قدّم التغذية الراجعة لهم.

الدرس الأول
أمن العتاد والبرمجيات ونظام التشغيل

رابط الدرس الرقمي

www.ien.edu.sa

مقدمة في أمن العتاد والبرمجيات ونظام التشغيل
Introduction to Hardware, Operating and Software System Security

أصبح أمن العتاد والبرمجيات وأنظمة التشغيل من التهديدات المحتملة مطلبًا ضروريًا في الأمن السيبراني. حيث تُشكّل هذه المُكوّنات الثلاثة بالإضافة إلى المعلومات والشبكات أساس أي نظام رقمي، ولذا فإن أمنها ضروري لضمان سلامة المُستخدمين وخصوصيتهم. سيناقش هذا الدرس طرائق أمن العتاد والبرمجيات ونظام التشغيل، ثم سيتم تناول أمن الشبكة في الدرس التالي.

أمن العتاد Hardware Security

يتضمّن أمن العتاد الحماية بالمُكوّنات المادية لنظام الحاسب مثل: المعالجات، والذاكرة، وأجهزة التخزين، كما يتضمّن اتّخاذ تدابير معيّنة لمنع الوصول غير المُصرّح به أو التخريب المتعمد. وحماية الأجهزة من التّلف الناتج عن العوامل البيئية، أو اختلالات التيار الكهربائي، وغير ذلك من المخاطر المحتملة. تتضمّن بعض تقنيات أمن العتاد الشائعة: استخدام عمليات بدء تشغيل آمنة (Secure Boot Processes)، واستخدام وحدات المنصّة الموثوقة (Trusted Platform Modules – TPMs) للتشفير، والأمانة بمفاتيح أمن عتادية (Hardware Security Keys) لعمليات المصادقة.

التهديدات الرئيسة لأنظمة العتاد:

- الهجمات المادية (Physical Attacks): تشمل الوصول غير المُصرّح به إلى مكوّنات الأجهزة أو تغييرها أو سرقتها.
- المُكوّنات المزيفة (Counterfeit Components): تشمل إدخال مُكوّنات أجهزة زائفة أو مقلدة، أو أجهزة ذات أداء دون المستوى المطلوب في سلسلة توريد الأجهزة، مما قد يُعرّض الأمن للخطر.
- أحصنة طروادة العتادية (Hardware Trojans): هي دوائر إلكترونية أو مُكوّنات ضارة مخفيّة داخل العتاد لديها القدرة على اختراق النظام أو تسريب البيانات الحساسة.
- هجمات القنوات الجانبية (Side-Channel Attacks): هي الهجمات التي تعتمد على المعلومات التي يُمكن الحصول عليها من العتاد مثل: استهلاك الطاقة، أو الإشعاع الكهرومغناطيسي، أو التوقيت.

ممارسات الأمان لحماية أنظمة العتاد:

- عملية بدء التشغيل الآمنة (Secure Boot Process): التأكد من أن عملية بدء التشغيل تستخدم توقيعًا رقميًا للتحقق من موثوقية نظام التشغيل.
- وحدات المنصّة الموثوقة (TPMs): تضمين هذه الوحدات لتفعيل التشفير المبني على العتاد، والتخزين الآمن لمفاتيح التشفير.
- مفاتيح أمن عتادية (Hardware Security Keys): يتم فيها استخدام رموز العتاد (Hardware Tokens)، أو الأجهزة المبنيّة على الخصائص الحيوية للمصادقة متعددة العوامل (MFA).

51

وزارة التعليم
Ministry of Education
2023 - 1445

> يمكنك توجيه الطلبة لحل التمرينات الثاني والثالث والرابع؛ للتحقق من فهمهم للتهديدات التي يمكن أن تصيب عتاد الحاسب، وأنظمة التشغيل، والبرمجيات. وممارسات الأمان للحماية منها.

> انتقل إلى شرح تقنيات تصميم النظام الآمن، وقدّم لهم الأمثلة على لكل نوع.

> اشرح لهم نهج **الأمن من خلال التصميم** (Security by Design)، ووضّح أنه يُضمّن بروتوكولات الأمن في المنتج منذ البداية.

> انتقل لشرح نهج **الدفاع متعدد الطبقات** (Defense In-Depth)، ثم وضّح أبرز الاختلافات بينه وبين نهج الأمن من خلال التصميم.

> اشرح لهم نهج **البرمجة الآمنة** (Secure Programming)، ووضّح تطبيقاته من خلال الجدول (2.5).

> استمر في الشرح بتوضيح **مفاتيح المرور** (Passkeys) وأمن الأجهزة، وبيّن لهم أبرز التقنيات المستخدَمة فيها.

> أشِر إلى أهمية استخدام اسم مُستخدِم فريد وكلمة مرور قوية ومعقدة لحماية حسابات المُستخدِمين من التهديدات الشائعة.

البرمجة الآمنة Secure Programming

تتضمّن البرمجة الآمنة كتابة تعليمات برمجية خالية من الثغرات الأمنية وغيرَ قابلة للاستغلال، وتتضمّن استخدام تقنيات الترميز الآمن وأفضل الممارسات ومنهجيات التطوير لتقليل مخاطر وجود عيوب أمنية في البرمجيات. ويوضّح الجدول 2.5 السيناريوهات التي يتم فيها تطبيق تقنية البرمجة الآمنة.

جدول 2.5: تطبيقات الأمن بواسطة تقنية البرمجة الآمنة

السيناريو	التطبيق
تطوير تطبيق الويب	يقوم المُطوّرون بإنشاء تطبيق ويب جديد لنظام مصرفي. وفي هذا السياق قد تتضمّن البرمجة الآمنة التحقق من صحة الإدخال، واستخدام اتصالات آمنة ومشفرة باستخدام بروتوكول نقل النص التشعبي الآمن (HTTPS)، وتنفيذ إدارة دخول مناسبة إلى النظام.
تطوير تطبيق الهاتف الذكي	تُوجب البرمجة الآمنة على المُطوّرين العاملين في تطوير تطبيق جديد للهاتف الذكي خاص بالرعاية الصحية التأكد من عدم تخزين التطبيق البيانات الحساسة بشكل غير آمن على الجهاز، وتنفيذ ضوابط ومصول قوية، وتشفير جميع البيانات المنقولة بين التطبيق والخادم.

مفاتيح المرور وأمن الأجهزة Passkeys and Device Security

هناك العديد من الأدوات والتقنيات المُستخدمة لحماية الأجهزة وبياناتها، وقد أثبتت أبسط تدابير الأمن فعاليتها ضد الثغرات الأمنية، ومفاتيح المرور (Passkeys) أحد الأمثلة الحديثة على هذه التدابير. مفتاح المرور هو بيانات اعتماد رقمية تُمثّل مَحلّ كلمات المرور التقليدية، وتسمح للمُستخدمين بتسجيل الدخول إلى التطبيقات ومواقع الويب باستخدام مستشعرات البيانات الحيوية، أو رقم التعريف الشخصي (Personal Identification Number-PIN)، أو أنماط القفل (Patterns)، حيث تُوفر مفاتيح المرور حماية قوية ضد هجمات التصيد الإلكتروني، وتعمل بالطريقة نفسها سواء عند استخدام المتصفح أو أنظمة التشغيل، وتعتمد رغبةً المُستخدمين في تسجيل الدخول بخدمة مفتاح المرور، بساعدهم المتصفح أو نظام التشغيل في اختيار واستخدام مفتاح المرور الصحيح. سيطلب النظام من المُستخدمين إما فتح أجهزتهم باستخدام مستشعر البيانات الحيوية، أو رقم التعريف الشخصي (PIN) أو نمط القفل. وينبع ذلك التأكد من أن المُستخدم الشرعي هو مَنْ يُمكنه استخدام مفتاح المرور حصرًا. تستخدم مفاتيح المرور تشفير المفتاح العام (Public Key Cryptography)، مما يُقلّل من التهديدات المحتملة بطُرُقات البيانات. فعندما ينشئ المُستخدم مفتاح مرور لموقع أو لتطبيق، يتم إنشاء زوج مفاتيح، مفتاح عام وآخر خاص على جهازه. يُخزّن الموقع أو التطبيق المفتاح العام فقط الذي يُعدّ وحده عديم الفائدة للمهاجم، حيث لا يمكن اشتقاق المفتاح الخاص بالمُستخدم من البيانات المُخزنة على الخادم، وهو أمر مطلوب لإكمال المصادقة. ترتبط مفاتيح المرور بهوية موقع الويب أو التطبيق، وبذلك فهي لا تأثر من هجمات التصيد الإلكتروني. كما يضمن المتصفح ونظام التشغيل بأنه لا يمكن استخدام مفتاح المرور إلا في موقع الويب أو التطبيق الذان أنشأ لهما. ويسمح هذا الإجراء المُستخدمين من إمكانية تسجيل الدخول إلى موقع ويب مُتاح أو تطبيق مريف. أحد الأمثلة هو الهوية السريعة على الإنترنت (Fast Identity Online – FIDO2)، وهو معيار مصادقة مفتوح يدعم المصادقة دون كلمة مرور باستخدام البيانات الحيوية ومفاتيح الأمن الخارجية. ويوضّح الشكل 2.1 استخدام مفتاح المرور.

شكل 2.1: مصادقة الأجهزة المحمولة باستخدام مفتاح مرور

57

وزارة التعليم
Ministry of Education
2023 - 1445

- وجّه الطلبة لحل التمرينات الخامس والسادس والسابع؛ بهدف التأكد من فهمهم لتقنيات تصميم النظام الآمِن.
- وضّح لهم أهمية جدار حماية ويندوز، ثم اشرح طريقة تفعيله على الحاسب.
- استمر في شرح كيفية السماح لتطبيقات الموجودة على الحاسب بالوصول إلى الإنترنت.
- واصل الشرح بتوضيح أهم الأذونات للملفات والمجلدات على الحاسب، وكيفية تعديلها للتحكم في الوصول لملفات الحاسب، ومجلداته.
- أكّد على أكثر أذونات نظام ملفات التقنية الجديدة شيوعًا.
- في الختام يمكنك توجيه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.


تمرينات

1 حدّد الجملة الصحيحة والجملة الخاطئة فيما يلي.

	صحيحة	خاطئة
1. يتضمّن أمن العتاد الحماية بالمكوّنات المادية لنظام الحاسب.		
2. البرمجيات الضارة هي تعليمات برمجية ضارة يتم تشغيلها بحالةٍ أو حدث معيّن.		
3. تُستخدم تقنية البيئة المعزولة (Sandboxing) لعزل التطبيقات عن نظام التشغيل الرئيس.		
4. يشمل أمن البرمجيات تثبيت برامج مكافحة الفيروسات لاكتشاف البرامج الضارة وإزالتها.		
5. يتم استخدام عمليات بدء التشغيل الآمنة للتحقق من أصالة نظام التشغيل قبل بدء تشغيله.		
6. لا تعتمد مفاتيح المرور على استخدام البيانات الحيوية لمصادقة المُستخدم.		
7. يتضمن أمن البرامج الثابتة التأكد من توقيع تحديثات البرامج الثابتة بشكل مشفر وإتاحتها للأجهزة بشكلٍ آمن.		
8. يُستخدم التشفير لحماية البيانات الحساسة على أجهزة التخزين.		
9. يجب تثبيت تحديثات نظام التشغيل بصورة منتظمة لمعالجة أي ثغرات أمنية.		
10. الأمن من خلال التصميم نهج استباقي لتطوير أنظمة وتطبيقات آمنة من خلال دمج التدابير والاعتبارات الأمنية بعد إتمام عملية التطوير.		

63


5 قيّم فعالية تقنيات تصميم النظام الآمن المُستخدمة لحماية الأنظمة الرقمية.

6 اسرد بعض الأمثلة على تطبيقات عملية الأمن من خلال التصميم.

7 صف كيف تُستخدم مفاتيح المرور كطريقة مصادقة حديثة.

65

يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يتضمَّن أمن العتاد العناية بالمكوِّنات المادية لنظام الحاسب.	✓	
2. البرمجيات الضارة هي تعليمات برمجية ضارة يتم تشغيلها بحالةٍ أو حدث معيَّن.	✓	
3. تُستخدم تقنية البيئة المعزولة (Sandboxing) لعزل التطبيقات عن نظام التشغيل الرئيس.	✓	
4. يشمل أمن البرمجيات تثبيت برامج مكافحة الفيروسات لاكتشاف البرامج الضارة وإزالتها.	✓	
5. يتم استخدام عمليات بدء التشغيل الآمنة للتحقق من أصالة نظام التشغيل قبل بدء تشغيله.	✓	
6. لا تعتمد مفاتيح المرور على استخدام البيانات الحيوية لمصادقة المُستخدِم. يمكن استخدام البيانات الحيوية لمصادقة المُستخدِم.		✓
7. يتضمن أمن البرامج الثابتة التأكد من توقيع تحديثات البرامج الثابتة بشكل مشفر وإتاحتها للأجهزة بشكلٍ آمن.	✓	
8. يُستخدم التشفير لحماية البيانات الحساسة على أجهزة التخزين.	✓	
9. يجب تثبيت تحديثات نظام التشغيل بصورة منتظمة لمعالجة أي ثغرات أمنية.	✓	
10. الأمن من خلال التصميم نهج استباقي لتطوير أنظمة وتطبيقات آمنة من خلال دمج التدابير والاعتبارات الأمنيّة بعد إتمام عملية التطوير. يتم أخذ الأمن من خلال التصميم في الاعتبار أثناء عملية التطوير.		✓

يمكن تقديم إجابات إضافية من قبل الطلبة

2 قيِّم المخاطر المرتبطة بمكوِّنات العتاد القديم أو غير المدعومة.

- الهجمات المادية (Physical Attacks): تشمل الوصول غير المُصرَّح به إلى مكوِّنات الأجهزة أو تغييرها أو سرقتها.
- المُكوِّنات المزيفة (Counterfeit Components): تشمل إدخال مُكوِّنات أجهزة زائفة أو مقلدة، أو أجهزة ذات أداء دون المستوى المطلوب في سلسلة توريد الأجهزة، مما قد يُعرِّض الأمن للخطر.
- أحصنة طروادة العتادية (Hardware Trojans): هي دوائر إلكترونية أو مُكوِّنات ضارة مخفيَّة داخل العتاد لديها القدرة على اختراق النظام أو تسريب البيانات الحساسة.
- هجمات القنوات الجانبية (Side-Channel Attacks): هي الهجمات التي تعتمد على المعلومات التي يُمكن الحصول عليها من العتاد مثل: استهلاك الطاقة، أو الإشعاع الكهرومغناطيسي، أو التوقيت.

3 قارِن بين التحديات التي تواجه ضمان أمن العتاد وأمن أنظمة البرمجيات.

التحديات الرئيسة لحماية العتاد والبرمجيات	
التحدي	الوصف
أمن نظام العتاد	
العَبَث المادي بالأجهزة	حماية العتاد من الوصول المادي غير المُصرَّح به أو التغيير أو السرقة.
أمن سلسلة التوريد	ضمان أمن وسلامة مُكوِّنات العتاد في جميع مراحل سلسلة التوريد بدءًا من التصنيع إلى التشغيل.
الثغرات الأمنيّة للبرامج الثابتة	تحديد الثغرات الأمنيّة في البرامج الثابتة التي يُمكن للمهاجمين استخدامها لاختراق العتاد، ومعالجتها بشكل صحيح.
تَقادُم العتاد	التعامل مع مخاطر الأمن المرتبطة بمكوِّنات الأجهزة القديمة أو غير المدعومة.
أمن أنظمة البرمجيات	
تهديدات الثغرات الأمنيّة الصفرية	تحديد الثغرات الأمنيّة للبرامج التي لم تَكُن معروفة سابقًا، ومعالجتها قبل استغلالها من قِبَل المهاجمين.
تعقيدات البرمجيات	إدارة الحاجة المتزايدة لأنظمة برمجية أكثر تعقيدًا، والتي يُمكن أن تؤدي إلى ثغرات جديدة تجعل من الصعب تحقيق الأمن.
هجمات سلسلة توريد البرمجيات	تأمين سلسلة توريد البرمجيات ومكوِّناتها ضد الاختراقات التي تؤدي إلى إدخال نصوص برمجية ضارة أو إيجاد ثغرات أمنية في تلك البرمجيات.

يمكن تقديم إجابات إضافية من قبل الطلبة

4 حلِّل أفضل الممارسات الرئيسة لحماية أنظمة التشغيل.

- مصادقة المُستخدِم: تتطلب استخدام اسم مُستخدِم فريد، وكلمة مرور قوية ومُعقَّدة لكل حساب مُستخدِم.
- أذونات الملفات والمجلدات: هي إعداد ضوابط وصول مناسبة لتقييد الوصول إلى الملفات والمجلدات الحساسة.
- التشفير: يكون باستخدام أدوات تشفير مضمنة في نظام التشغيل لحماية البيانات الحساسة على أجهزة التخزين.
- جدار الحماية: تفعيل وإعداد جدار حماية لنظام التشغيل لمراقبة حركة بيانات الشبكة الواردة والصادرة من أو إلى نظام التشغيل والتحكم فيها.
- تحديثات نظام التشغيل العادية: من خلال تثبيت حِزم إصلاحات نظام التشغيل والتحديثات الأمنيّة لمعالجة الثغرات الأمنيّة.
- الإعدادات الأمنيّة الأساسية والتحصين: عن طريق تطبيق أفضل الممارسات والإعدادات الأمنيّة لنظام التشغيل للحدِّ من تأثير الهجمات المختلفة.

5 قيِّم فعالية تقنيات تصميم النظام الآمن المُستخدَمة لحماية الأنظمة الرقمية.

- من خلال دمج الأمن من خلال التصميم المتعمق والدفاع متعدد الطبقات في عملية التطوير، يمكن للمؤسسات إنشاء أنظمة أكثر أمانًا ومجهزة بشكل أفضل للحماية من مجموعة واسعة من التهديدات والهجمات.
- تتضمَّن البرمجة الآمنة كتابة تعليمات برمجية خالية من الثغرات الأمنيّة وغَيرَ قابلة للاستغلال، وتتضمَّن استخدام تقنيات الترميز الآمن وأفضل الممارسات ومنهجيات التطوير لتقليل مخاطر وجود عيوب أمنية في البرمجيات.
- من خلال تقييد الوصول باستخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات، لا يستطيع المهاجمون الحصول على السيطرة الكاملة، وهو أمر ضروري لحماية النظام من التهديدات المحتملة.
- مفتاح المرور هو بيانات اعتماد رقمية تَحلُّ مَحَلَّ كلمات المرور التقليدية، وتسمح للمُستخدمين بتسجيل الدخول إلى التطبيقات ومواقع الويب باستخدام مستشعرات البيانات الحيوية، أو رقم التعريف الشخصي (PIN)، أو أنماط القفل (Patterns)، حيث تُوفِّر مفاتيح المرور حماية قوية ضد هجمات التصيد الإلكتروني، وتعمل بالطريقة نفسها سواء عند استخدام المتصفح أو أنظمة التشغيل.

يمكن تقديم إجابات إضافية من قبل الطلبة

6 اسرُد بعض الأمثلة على تطبيقات عملية الأمن من خلال التصميم.

- تطوير موقع الويب مع الأخذ بعين الاعتبار الأمن من خلال التصميم: عند تطوير موقع جديد للتجارة الإلكترونية، يقتضي الأمن من خلال التصميم استخدام ممارسات الترميز الآمنة، والتحقق من صِحّة إدخال البيانات لمنع حقن النصوص البرمجية بلغة SQL أو هجمات البرمجة العابرة للمواقع، وتنفيذ مصادقة قوية للمُستخدِم وضوابط للوصول من البداية.

- تطوير الخدمات السحابية مع الأخذ بعين الاعتبار الأمن من خلال التصميم: عند تطوير الخدمات السحابية، قد تتضمَّن أفضل الممارسات استخدام واجهات برمجة التطبيقات الآمنة، وآليات مصادقة قوية، والتحكم بالوصول، وتقنيات تشفير البيانات المدمجة.

7 صِف كيف تُستخدَم مفاتيح المرور كطريقة مصادقة حديثة.

مفتاح المرور هو عبارة عن بيانات اعتماد رقمية تحل محل كلمات المرور التقليدية وتسمح للمُستخدِمين بتسجيل الدخول إلى التطبيقات ومواقع الويب باستخدام أجهزة الاستشعار الحيوية أو أرقام التعريف الشخصية أو أنماط القفل. حيث توفر مفاتيح المرور حماية قوية ضد هجمات التصيد الالكتروني، كما أنها موحدة عبر المتصفحات وأنظمة التشغيل. وعندما يريد المُستخدِمون تسجيل الدخول بخدمة مفتاح المرور، سيساعدهم المتصفح أو نظام التشغيل الخاص بهم في اختيار واستخدام مفتاح المرور الصحيح. سيطلب النظام من المُستخدِمين إلغاء قفل أجهزتهم باستخدام مستشعر البيانات الحيوية أو رقم التعريف الشخصي أو نمط القفل. وهذا يضمن أن المالك الشرعي فقط يمكنه استخدام مفتاح المرور. تستخدم مفاتيح المرور تشفير المفتاح العام؛ مما يقلل من تهديدات المحتملة لاختراق البيانات. فعندما يقوم مُستخدِم بإنشاء مفتاح مرور لموقع أو تطبيق، يؤدي ذلك إلى إنشاء زوجَيْ مفاتيح (عام، وخاص) على جهازه.

الموقع فقط هو الذي يخزن المفتاح العام، لكن هذا وحده لا فائدة منه للمهاجم. حيث لا يمكن للمهاجم استخلاص المفتاح الخاص للمُستخدِم من البيانات المخزنة على الخادم، وهو أمر مطلوب لإكمال المصادقة.

أمن الشبكات والويب

وصف الدرس

الهدف العام من الدرس هو التعرف على هياكل الشبكات وتقنيات الويب في الأمن السيبراني، وتمييز تقنيات أمن الشبكة والويب، ومراقبة الشبكة والتقاط حِزم البيانات، بالإضافة لتحليل مخرجات برنامج واير شارك، والاتصال بخدمة الشبكة الافتراضية الخاصة من نظام تشغيل ويندوز.

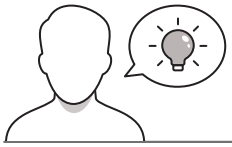
أهداف التعلُّم

- معرفة هياكل الشبكات وتقنيات الويب في الأمن السيبراني.
- تمييز تقنيات أمن الشبكة والويب.
- مراقبة الشبكة والتقاط حِزم البيانات.
- تحليل مخرجات برنامج واير شارك.
- الاتصال بخدمة الشبكة الافتراضية الخاصة من نظام تشغيل ويندوز.

الدرس الثاني	
الوحدة الثانية: الحماية والاستجابة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الثاني: أمن الشبكات والويب	4

نقاط مهمَّة

- قد يصعب على بعض الطلبة التمييز بين المحوِّلات والموجِّهات، بيّن لهم الفرق مستعينًا بنظام الشبكات الموجود في المدرسة.
- قد لا يدرك بعض الطلبة المخاطر الأمنيّة المتنوعة التي تهدد الأجهزة والبيانات عند استخدام شبكات الواي فاي (WiFi) اللاسلكية العامة، بيّن لهم أفضل الممارسات لحماية الأجهزة عند استخدامها.

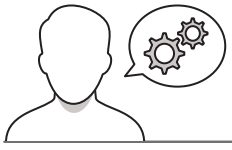


التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- ماذا تعرفون عن البروتوكولات في الشبكات؟
- هل سبق أن سمعتم عن **الشبكة الافتراضية الخاصة** (VPN)؟ وإلى ماذا يُشير هذا الاختصار؟
- هل تنصح بالاتصال شبكة الواي فاي اللاسلكية العامة؟ ولماذا؟



خطوات تنفيذ الدرس

> في البداية ناقش الطلبة حول مفهوم هياكل الشبكات، وبيّن أهميتها، ثم قدّم الأمثلة عليها.

> وضّح لهم مفاهيم الشبكات الأساسية، وعرّفهم بمصطلحاتها الإنجليزية، وبيّن أهمية ذلك.

> اشرح لهم مكونات الشبكات الأساسية، والمهمة التي يقوم بها كل منها.

> انتقل إلى شرح بروتوكولات الشبكات الأساسية، وبيّن لهم الدور الذي يقوم به كل برتوكول منها.

> وجّه الطلبة لحل التمرين الثاني؛ للتحقق من فهمهم لبروتوكولات الشبكات الأساسية.

> اشرح للطلبة تقنيات أمن الشبكات والويب، ثم وضّح لهم أفضل الممارسات لحماية الأجهزة عند استخدام شبكة الواي فاي اللاسلكية العامة.


الدرس الثاني
أمن الشبكات والويب

هياكل الشبكات وتقنيات الويب في الأمن السيبراني
Network Structures and Web Technologies in Cybersecurity

يُعدّ فهم هيكلية الشبكات وتقنيات الويب أمرًا بالغ الأهمية في الأمن السيبراني. حيث ترتبط هذه العناصر بطبيعة التهديدات، وبالتدابير الوقائية التي يُمكن اتخاذها للحدّ منها. وتتكوّن الشبكات من أجهزة مترابطة تتبادل المعلومات مع بعضها البعض، بينما تتيح تقنيات الويب إنشاء ومشاركة المحتوى والتطبيقات عبر الإنترنت. يُمكن وصف الإنترنت بأنه شبكة مكوّنة من مجموعة من الشبكات. ومع ازدياد عدد الأجهزة والخدمات المُدمَجة عبر الويب، فإن هذه الأنظمة تزداد تعقيدًا. وكذلك تزداد نقاط ضعفها. تؤثر هيكلية الشبكات وتقنيات الويب بشكل مباشر على أنواع التهديدات التي يُمكن مواجهتها في مجال الأمن السيبراني، فعلى سبيل المثال، قد تواجه الشبكات هجمات رفض الخدمة الموزع (DDoS) التي بدورها تؤثر على الخدمات وعملائها من خلال إغراقها بحركة بيانات ضخمة. وقد تتعرض تقنيات الويب كذلك للتهديدات مثل هجمات البرمجة المُعبرة للمواقع (XSS) وهجمات حقن النصوص البرمجية بلغة SQL (SQL injection)، حيث يستغل المتسللون ثغرات تطبيقات الويب للوصول غير المُصرّح به إلى البيانات الحساسة. تُحدّد هيكلية الشبكات وتقنيات الويب المُستخدمة طبيعة التدابير الوقائية التي يُمكن استخدامها لحمايتها، فعلى سبيل المثال، يُمكن لتجزئة الشبكة عزل الأنظمة الهامة وتقليل نطاق الهجوم المحتمل. وفي المقابل يُمكن لأنظمة كشف التسلّل (IDSs) ومُدران الحماية المساعدة في مراقبة تدفق حركة البيانات داخل الشبكة وخارجها والتحكم بها. يُمكن أن تساعد ممارسات البرمجة الآمنة والمناسبة في تقنيات الويب مثل: التحقق من صحة الأدخال، ومعالجة الأخطاء المناسبة في منع استغلال الثغرات الأمنيّة. فيما يلي عرض لأهم المفاهيم الأساسية الخاصة بالشبكات وتقنية الويب المُؤثرة على تهديدات الأمن السيبراني وتدابير الحماية.

مفاهيم الشبكات الأساسية Fundamental Networking Concepts

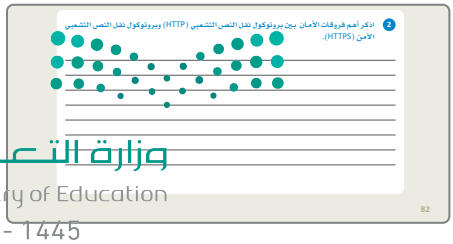
مخططات الشبكة (Network Topologies):
هي الترتيب المادي أو المنطقي للأجهزة في الشبكة، وتشمل الهياكل الشائعة للشبكات: الهيكل النجمي والحلقي والخطي والشبكي والهجين.

أجهزة الشبكة (Network Devices):
هي مكوّنات الأجهزة الأساسية التي تُسهّل الاتصال داخل الشبكات مثل: المحوّلات (Switches) والموجّهات (Routers) وجُدران الحماية (Firewalls) ونقاط الوصول (Access Points).

وسائط النقل (Transmission Media):
هي الوسائل المادية أو اللاسلكية التي يتم من خلالها نقل البيانات بين الأجهزة في الشبكة. وتشمل كابلات الشبكة المحلية (Ethernet) مثل: الكابلات المزدوجة أو الكابلات المحورية أو الألياف الضوئية، والتقنيات اللاسلكية مثل: الواي فاي (Wi-Fi) أو البلوتوث (Bluetooth) أو الشبكات الخلوية (Cellular Networks).

بروتوكولات الشبكة (Network Protocols):
هي مجموعة قواعد وتعريفات تحدّد كيفية اتصال الأجهزة وتبادل المعلومات داخل الشبكة. وتعمل البروتوكولات في طبقات مختلفة من نموذج الربط البيني للأنظمة المفتوحة (Open Systems Interconnection – OSI) أو نماذج بروتوكول IP / TCP. وتتضمن الأمثلة بروتوكولات IP، UDP، TCP، FTP، HTTP/S.

66


2 اذكر أهم فروقات الأمان بين بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل النص التشعبي الآمن (HTTPS).

82

> يمكنك توجيه الطلبة لحل التمرينات الثالث والرابع والخامس والسادس؛ للتحقق من فهمهم لتقنيات أمن الشبكات والويب.


3 اشرح كيفية استخدام المناطق العازلة (DMZs) لحماية الشبكات الداخلية من التهديدات الخارجية.

4 قيّم فعالية الشبكات الافتراضية الخاصة (VPNs) في الحفاظ على خصوصية المُستخدم.

83


5 وضّح كيفية استخدام جُدران الحماية وأنظمة كشف التسلُّل (IDSs) لحماية الشبكات من الهجمات.

6 اشرح الفرق بين نظام كشف التسلُّل المُستند إلى الشبكة (NIDS)، ونظام كشف التسلُّل المُستند إلى المُضيف (HIDS).

84

> واصل الشرح بتوضيح مفهوم مراقبة الشبكة والتقاط حِزم البيانات، ثم اشرح لهم خصائص برنامج **وايرشارك** (Wireshark) كأحد أدوات تحليل حِزم البيانات الأكثر شيوعًا.

> اشرح للطلبة واجهة برنامج وايرشارك، وكيفية مراقبة الشبكة من خلاله.

> وضّح لهم اللوحات الثلاث التي تتدفق من خلالها حِزم البيانات، وتفاصيل كل حزمة.

> اشرح كيفية تحليل فحص وايرشارك، والتعرف على مدلولات حركة البيانات المسجلة للشبكة.

> وضّح لهم كيفية كشف نشاط مريب على الشبكة، ثم اشرح طريقة تحليل تَدفُّق البيانات بخيار **معلومات الخبير** (Expert Information).

> استمر في شرح الدرس ووضّح الاتصال بخدمة الشبكة الافتراضية الخاصة من نظام تشغيل ويندوز، وطريقة تفعيلها.


مراقبة الشبكة والتقاط حزم البيانات
Network Monitoring and Packet Sniffing

تُوجد أدوات مفيدة تُستخدم لمراقبة حركة بيانات الشبكة وللتقّط وتحليل الحزم التي يتم إرسالها عبرها، حيث يتم تنفيذ هذه الإجراءات بواسطة أدوات تُسمى مُحلِّلات حزم البيانات (Packet Analyzers). ويُعدُّ برنامج وايرشارك (Wireshark) أحد أكثر أدوات تحليل حزم البيانات شيوعًا.

وايرشارك (Wireshark) هو مُحلِّل حزم بيانات مفتوح المَصدر يُستخدم لفحص تفاصيل حركة البيانات على عدة مستويات، بدءًا من مستوى معلومات الاتصال وحتى مستوى معلومات الحزم الفردية. كما يتيح لمسؤول الشبكة الحصول على معلومات تتعلق بالحزم الفردية مثل: وقت الإرسال، والمصدر، والوجهة، ونوع البروتوكول. وبيانات رأس الحزمة التي يُمكن أن تكون مهمة جدًا لتقييم مشكلات الأمن وتشخيصها. يُمكنك تنزيل البرنامج وتثبيته من الرابط التالي:
https://www.wireshark.org/download.html

شكل 2.8: زر الاستجابة السريعة (QR) لتنزيل برنامج وايرشارك

مراقبة الشبكة باستخدام وايرشارك Monitoring a Network with Wireshark

سنتعرف الآن على واجهة مُحلِّل الشبكة وايرشارك (Wireshark).

لمراقبة الشبكة باستخدام وايرشارك:
1. افتح تطبيق وايرشارك واعرض قائمة Available Networks (الشبكات المتاحة).
2. اضغط على أمر Capture (الالتقاط).
3. من تلك Capture (الالتقاط)، اضغط على الشبكة التي تريد مراقبتها.
4. اضغط على زر Start (بدء).
5. راقب تدفق حزم البيانات في الشبكة.
6. اضغط على زر Stop (إيقاف) لإنهاء مراقبة الشبكة.

1
2
يتم هنا عرض جميع واجهات الشبكة

70

> يمكنك توجيه الطلبة لحل التمرينات السابع والثامن والتاسع؛ للتحقق من فهمهم لمراقبة الشبكة والتقاط حِزم البيانات، وتحليل مُخرَجات واير شارك.

> في الختام يمكنك توجيه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.

تمرينات

1

حدد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. تتضمَّن وسائط نقل الشبكة الكابلات المزدوجة والمحورية وكابلات الألياف الضوئية.		
2. المُوجِّهات هي المسؤولة عن توجيه حركة البيانات داخل الشبكة المحلية (LAN).		
3. الهجوم البرمجي العابر للمواقع (XSS) نوعٌ من الهجمات المبنية على مواقع الويب.		
4. بروتوكول الإنترنت الآمن (IPSec) هو بروتوكول شبكة شائع الاستخدام.		
5. تتوفَّر جُدران الحماية (Firewalls) على شكل برامج أو على شكل عتاد.		
6. تُراقِب أنظمة كشف التسلُّل (IDS) عمليات نقل الملفات.		
7. بروتوكول طبقة المنافذ الآمنة (SSL) هو بروتوكول لتشفير البيانات أثناء نقلها.		
8. يقوم نظام أسماء النطاقات (DNS) بترجمة عناوين بروتوكول الإنترنت (IP) إلى أسماء نطاقات يُمكن قراءتها.		
9. يُستخدم واير شارك (Wireshark) في عمليات التقاط حِزم البيانات.		

82

7 التقاط وتحليل حركة بيانات الشبكة:

- افتح واير شارك (Wireshark) وحدِّد واجهة الشبكة الخاصة بك، وابدأ بالتقاط الحِزَم.
- تصفَّح الإنترنت لبضع دقائق، عن طريق فتح بعض مواقع الويب، ومشاهدة مقطع فيديو، وما إلى ذلك.
- توقَّف عن التقاط الحزم واحفظ البيانات.
- حلِّل حركة البيانات، واستخرج بعض المعلومات مثل المصدر IP/Port (بروتوكول الإنترنت / المنفذ)، والوجهة IP/Port (بروتوكول الإنترنت / المنفذ) و Capture time (وقت الالتقاط).

8 تحليل طلب بروتوكول اقتران العناوين (ARP):

- التقط صورة جديدة للشبكة المحلية (Ethernet) الخاصة بك.
- قم بتصفية نتائج بروتوكول اقتران العناوين (ARP) بكتابة "arp" في شريط filter (التصفية).
- حلِّل النتائج. كم عدد طلبات بروتوكول اقتران العناوين (ARP) الموجودة؟ وهل يُمكنك تحديد عناوين التحكم بالنفاذ للوسط (MAC) للمصدر والوجهة؟

9 الكشف عن نشاط غير طبيعي في الشبكة بواسطة واير شارك (Wireshark)

- حمِّل ملف Scan_results.pcapng الذي سيمنحه لك معلِّمك.
- استخدم علامة تبويب Expert Information (معلومات الخبير) للعثور على أي مشكلات محتملة أو نشاطات غير اعتيادية في الشبكة.
- ابحث عن أي ملاحظات غير طبيعية وحاول تحديد سببها. وهل توجد إشارة على وجود تهديد أمني محتمل؟

85

يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. تتضمَّن وسائط نقل الشبكة الكابلات المزدوجة والمحورية وكابلات الألياف الضوئية.	✓	
2. المُوجِّهات هي المسؤولة عن توجيه حركة البيانات داخل الشبكة المحلية (LAN). المُوجِّهات مسؤولة عن نقل حِزم البيانات بين الشبكات المختلفة		✓
3. الهجوم البرمجي العابر للمواقع (XSS) نوعٌ من الهجمات المبنية على مواقع الويب.	✓	
4. بروتوكول الإنترنت الآمن (IPSec) هو بروتوكول شبكة شائع الاستخدام.	✓	
5. تَتوفَّر جُدران الحماية (Firewalls) على شكل برامج أو على شكل عتاد. جدران الحماية (Firewalls) هي آليات وأجهزة برمجية.		✓
6. تُراقِب أنظمة كشف التسلُّل (IDS) عمليات نقل الملفات.	✓	
7. بروتوكول طبقة المنافذ الآمنة (SSL) هو بروتوكول لتشفير البيانات أثناء نقلها.	✓	
8. يقوم نظام أسماء النطاقات (DNS) بترجمة عناوين بروتوكول الإنترنت (IP) إلى أسماء نطاقات يُمكن قراءتها.	✓	
9. يُستخدم واير شارك (Wireshark) في عمليات التقاط حِزم البيانات.	✓	

2 اذكر أهم فروقات الأمان بين بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل النص التشعبي الآمن (HTTPS).

- بروتوكول نقل النص التشعبي (HTTP): يستخدم لنقل المحتوى المبني على الويب بين عميل (على سبيل المثال متصفح الويب) وخادم باستخدام اتصال بواسطة بروتوكول التحكم بالنقل (TCP)، مما يتيح تبادل النصوص والصور وعناصر الوسائط المتعددة الأخرى.

- بروتوكول نقل النص التشعبي الآمن (HTTPS): إصدار مشفر من بروتوكول نقل النص التشعبي (HTTP) يستخدم بروتوكول أمن طبقة النقل/ بروتوكول طبقة المنافذ الآمنة (SSL / TLS) بدلًا من استخدام بروتوكول التحكم بالنقل (TCP) مباشرة، ويتم استخدامه حاليًا في غالبية خدمات الإنترنت..

يمكن تقديم إجابات إضافية من قبل الطلبة

3 اشرح كيفية استخدام المناطق العازلة (DMZs) لحماية الشبكات الداخلية من التهديدات الخارجية.

المنطقة العازلة **(DMZ)** هي جزء من الشبكة يقع بين شبكة المؤسسة الداخلية والشبكة الخارجية غير الموثوق بها، مثل الإنترنت، وتم تصميم هذه المنطقة لتوفير طبقة إضافية من الحماية، وذلك بعَزل الخدمات التي يجب الوصول إليها عبر الإنترنت مثل: خوادم الويب أو خوادم البريد الإلكتروني عن الشبكة الداخلية للمؤسسة، ومن خلال وضع الخدمات التي يتم الوصول إليها عبر الإنترنت في منطقة عازلة **(DMZ)**، يتم احتواء نطاق أي هجمات أو ثغرات محتملة داخل تلك المنطقة والحَدِّ من احتمالات تأثيرها على الشبكة الداخلية، ويسمح هذا التكوين للمؤسسات بالحفاظ على مستوى أعلى من الأمن لأنظمتها وبياناتها الهامة.

4 قيِّم فعالية الشبكات الافتراضية الخاصة (VPNs) في الحفاظ على خصوصية المُستخدِم.

الشبكة الافتراضية الخاصة **(VPN)** هي تقنية تُنشئ اتصالًا آمنًا ومشفّرًا بين جهاز المُستخدِم وشبكة أخرى بعيدة غالبًا عبر الإنترنت، وتحمي الشبكات الافتراضية الخاصة سرية البيانات المنقولة وسلامتها بين جهاز المُستخدِم والشبكة البعيدة، مما يضمن بقاء المعلومات الحساسة مُؤمَّنة حتى عند إرسالها عبر شبكات غير آمنة.

توفِّر الشبكات الافتراضية الخاصة **(VPNs)** ميزات إضافية مثل: تجاوز القيود الجغرافية، وحماية خصوصية المُستخدِم، والسماح بالوصول عن بُعد إلى الشبكات الآمنة. يتم استخدام هذه التقنيات بشكل شائع من قِبل الشركات والأفراد على حدٍّ سواء للحفاظ على الأمن والخصوصية أثناء استخدام الإنترنت.

يمكن تقديم إجابات إضافية من قبل الطلبة

5 وضِّح كيفية استخدام جُدران الحماية وأنظمة كشف التسلُّل (IDSs) لحماية الشبكات من الهجمات.

- جدران الحماية: تراقب وتتحكم في حركة بيانات الشبكة الواردة والصادرة بناءً على قواعد أمن محدَّدة مسبقًا، وتحمي الشبكات الداخلية من الوصول غير المُصرَّح به والهجمات السيبرانية المحتملة.
- أنظمة كشف التسلُّل (IDSs) هي تقنية أمنية تراقب حركة البيانات في الشبكة بحثًا عن أي مؤشرات أو دلائل على وجود نشاط ضار أو اختراق أمني في الشبكة وأجهزتها. يُمكن لأنظمة كشف التسلُّل إصدار تنبيهات عند اكتشاف تهديدات محتملة، مما يسمح لمسؤولي الشبكة بالاستجابة بشكلٍ سريع، والعمل على إيقاف الهجوم أو الحد من تأثيره.

6 اشرح الفرق بين نظام كشف التسلُّل المُستند إلى الشبكة (NIDS)، ونظام كشف التسلُّل المُستند إلى المُضيف (HIDS).

- نظام كشف التسلُّل المُستند إلى الشبكة (NIDS): يُحلِّل هذا النوع من الأنظمة حركة بيانات الشبكة، ويبحث عن الأنماط المشبوهة أو أي مؤشرات للوصول غير المُصرَّح به.
- نظام كشف التسلُّل المُستند إلى المُضيف (HIDS): يتم تثبيت هذا النوع من نظام كشف التسلُّل (IDS) على أجهزة مستقلة مثل: الخوادم أو حاسبات محطات العمل، ويراقب هذا النظام نشاط النظام المحلي بحثًا عن أي مؤشرات اختراق أو وصول غير مُصرَّح به.

يمكن تقديم إجابات إضافية من قبل الطلبة

7 التقاط وتحليل حركة بيانات الشبكة:

- افتح وايرشارك (Wireshark) وحدِّد واجهة الشبكة الخاصة بك، وابدأ بالتقاط الحِزَم.
- تصفَّح الإنترنت لبضع دقائق، عن طريق فتح بعض مواقع الويب، ومشاهدة مقطع فيديو، وما إلى ذلك.
- تَوقَّف عن التقاط الحِزم واحفظ البيانات.
- حَلِّل حركة البيانات، واستخرج بعض المعلومات مثل المَصدر IP/Port (بروتوكول الإنترنت / المَنفذ)، والوِجهة IP/Port (بروتوكول الإنترنت / المَنفذ) و Capture time (وقت الالتقاط).

تلميح: **وقت الالتقاط** (Capture time) هو الفرق في عمود **الوقت** (Time) بين الصف الأول والأخير.

في هذه الحالة هو 0.000000 و50.248869 فيكون 50.2 ثانية.

تمت زيارة موقع **الهيئة السعودية للبيانات والذكاء الاصطناعي** (SDAIA) وموقع **الهيئة الوطنية للأمن السيبراني** (NCA) في هذه الصورة.

في جميع الحالات، فإن عنوان **بروتوكول الإنترنت للمَصدر** (Source IP) هو 199.0.0.27 ومَنفذ المَصدر له نطاق من القيم.

بالنسبة لموقع **الهيئة السعودية للبيانات والذكاء الاصطناعي** (SDAIA)، فإن عنوان **بروتوكول الإنترنت للوِجهة** (Destination IP) هو 176.105.151.12 ومَنفذ الوِجهة هو 443.

بالنسبة لموقع **الهيئة الوطنية للأمن السيبراني** (NCA)، فإن عنوان **بروتوكول الإنترنت للوِجهة** (Destination IP) هو 78.93.109.88 ومَنفذ الوِجهة هو 443.

يمكنك تنزيل ملف الالتقاط هنا:

https://bl-xtrransfer.s3.amazonaws.com/KSA/G12/CYB/U2/L2/U2_L2_EXERCISE_Scan.pcapng

يمكن تقديم إجابات إضافية من قبل الطلبة

8 تحليل طلب بروتوكول اقتران العناوين (ARP):

- التقط صورة جديدة للشبكة المحلية (Ethernet) الخاصة بك.
- قُم بتصفية نتائج بروتوكول اقتران العناوين (ARP) بكتابة "arp" في شريط filter (التصفية).
- حَلِّل النتائج. كم عدد طلبات بروتوكول اقتران العناوين (ARP) الموجودة؟ وهل يُمكنك تحديد عناوين التحكم بالنفاذ للوسط (MAC) للمَصدر وللوِجهة؟

تلميح: تم استخدام ملف Scan_results.pcapng مرة أخرى.

هناك 52 طلب **برتوكول اقتران العناوين** (ARP).

عناوين **مصدر التحكم بالنفاذ للوسط** (Source MAC):

HewlettP_a1:30:ee

HewlettP_a4:04:b8

Dell_9c:e5:c3

Dell_5e:92:58

Microsof_0a:8a:0b

Dell_f0:82:81

HuaweiTe_74:e8:fc

ICPElect_f4:89:1a

G-ProCom_6c:c1:21

عناوين وِجهة **التحكم بالنفاذ للوسط** (Destination MAC):

Broadcast

Dell_5e:92:58

Dell_9c:e5:c3

Dell_f0:82:81

IntelCor_5c:ee:a5

00:00:00_00:00:00

G-ProCom_6c:c1:21

يمكن تقديم إجابات إضافية من قبل الطلبة

9 الكشف عن نشاط غير طبيعي في الشبكة بواسطة واير شارك (Wireshark)

- حمِّل ملف Scan_results.pcapng الذي سيمنحه لك معلّمك.
- استخدم علامة تبويب Expert Information (معلومات الخبير) للعثور على أي مشكلات محتملة أو نشاطات غير اعتيادية في الشبكة.
- ابحث عن أي ملاحظات غير طبيعية وحاول تحديد سببها، وهل توجد إشارة على وجود تهديد أمني محتمل؟

تلميح: في نافذة **معلومات الخبير** (Expert Information) تُعدُّ الرسائل التي تحتوي على **تحذير** (Warning) مشكلات محتملة، حيث يتم تمييزها بواسطة برنامج **واير شارك** (Wireshark) كأنماط تشبه بداية الهجوم السيبراني. التهديدات الأمنية المحتملة هي:

إعادة ضبط الاتصال (Connection Reset - RST): قد يشير الارتفاع المفاجئ في حِزم **إعادة ضبط الاتصال** (RST) في سياق غير عادي (على سبيل المثال، أثناء نقل البيانات المستمر) إلى هجوم إعادة تعيين **برتوكول التحكم بالنقل** (TCP)، فقد يحاول أحد المهاجمين تعطيل الاتصال.

إعادة إرسال استعلام نظام أسماء النطاقات (DNS Query Retransmission): يمكن أن تكون عمليات إعادة الإرسال المتعددة إشارة إلى هجوم تضخيم **نظام أسماء النطاقات** (DNS) أو قد تعني أن خادم **نظام أسماء النطاقات** (DNS) يتعرض للضغط، ربما كجزء من هجوم **حجب الخدمة الموزع** (DDoS).

التحليل الجنائي الرقمي والاستجابة للحوادث

وصف الدرس

الهدف العام من الدرس هو التعرف على **التحليل الجنائي الرقمي** (Digital Forensics - DF) و**الاستجابة للحوادث** (Incident Response - IR)، بالإضافة لتحليل أنشطة الويب على الجهاز.

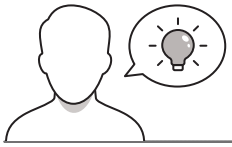
أهداف التعلُّم

- معرفة التحليل الجنائي الرقمي والاستجابة للحوادث.
- تحليل أنشطة الويب على الجهاز.

الدرس الثالث	
الوحدة الثانية: الحماية والاستجابة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الثالث: التحليل الجنائي الرقمي والاستجابة للحوادث	4

نقاط مهمَّة

- قد يظن بعض الطلبة أن التحليل الجنائي الرقمي يُستخدم لقضايا النشاط الإجرامي فقط، بيّن لهم أنه قد يُستخدم في الإجراءات القانونية، وفي التحقيقات الداخلية للشركات، وكذلك أنواع أخرى من التحقيقات الرقمية.
- قد يخلط بعض الطلبة بين مراحل سلسلة الهجوم السيبراني، وضّح لهم ما يحدث في كل مرحلة، ثم قدّم مثالًا واحدًا يضم كل تلك المراحل؛ ليسهُل عليهم التمييز بينها.



التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- هل سبق أن سمعتم بفِرَق **الاستجابة لحوادث أمن الحاسب** (Computer Security Incident Response Teams – CSIRTs)؟ وما مهمتها؟
- ما أنواع متصفحات الإنترنت التي تستخدمونها؟
- هل سبق لكم استخدام **متصفح دي بي** (DB Browser)؟

خطوات تنفيذ الدرس

في البداية ناقش الطلبة حول مفهوم التحليل الجنائي الرقمي والاستجابة للحوادث، ووضّح ما يُركز عليه كأحد فروع الأمن السيبراني.

> وضّح لهم مفهوم سلسلة الهجوم السيبراني، وبيّن أهمية معرفتها في عملية التحليل الجنائي الرقمي والاستجابة للحوادث.

> انتقل إلى شرح مراحل سلسلة الهجوم السيبراني، ووضّح ما يقوم به المهاجمون في كل مرحلة، ويمكنك تقديم مثال واحد يشتمل على كل تلك المراحل؛ ليسهُل على الطلبة تمييزها.

> اشرح لهم عمليات التحليل الجنائي الرقمي، ووضّح ما تشمله كل عملية منها.

> اشرح للطلبة الخطوات التي تمر بها عملية التحليل الجنائي الرقمي، وما يتم في كل مرحلة.

> وضّح لهم أيضًا الخطوات التي تمر بها عملية الاستجابة للحوادث النموذجية، وبيّن الهدف من كل مرحلة.

الدرس الثالث

التحليل الجنائي الرقمي والاستجابة للحوادث

مُقدّمة في التحليل الجنائي الرقمي والاستجابة للحوادث

Introduction to Digital Forensics (DF) and Incident Response (IR)

يُعدُّ التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) أحد فروع الأمن السيبراني المهمة المُرتكزة على تحديد الهجمات السيبرانية، والتحقيق فيها، واحتوائها، وتجاوزها. وتوفير المعلومات للقضايا القانونية أو التحقيقات الرقمية الأخرى. وتتكون هذه الخدمات من مُكوّنين رئيسين:

التحليل الجنائي الرقمي (Digital Forensics):

بصفته حقلًا استقصائيًا في علم التحليل الجنائي، يتضمّن التحليل الجنائي الرقمي عمليات جمع الأدلة الرقمية وتحليلها وتقديمها على أنظمة الحاسب، أو أجهزة الشبكة، أو الهواتف المحمولة، أو الأجهزة اللوحية. ويُمكن أن تساعد هذه الأدلة في الكشف عن حقيقة الأحداث التي حدثت على هذه الأجهزة. بدءًا بالنحو التحليل الجنائي الرقمي يطلق واسعة الإجراءات القانونية، والاستقصاءات التنظيمية، وفي التحقيقات الداخلية للشركات. وفي قضايا التشاط الإجرامي. وكذلك أنواع أخرى من التحقيقات الرقمية.

الاستجابة للحوادث (Incident Response):

تغطي الاستجابة للحوادث أيضًا قضايا التحقيق. ولكنها تُركّز بشكل خاص على معالجة الحوادث الأمنيّة. وفي هذه الحالات يقوم المُحقّقون بإجراءات مختلفة. يتعلّق بعضها بالاحتواء والتعامل للاستجابة بشكل فعّال للوضع القائم.

يؤدي كل من التحليل الجنائي الرقمي والاستجابة للحوادث أدوارًا حاسمة في الكشف عن المخاطر المحيطة بالأحداث الرقمية ومعالجة الحوادث الأمنيّة المحتملة لضمان أمن الأنظمة والبيانات الرقمية وسلامتها.

سلسلة الهجوم السيبراني (Cyber Kill Chain):

تُستخدم منهجية سلسلة الهجوم السيبراني لفهم وتحليل الهجمات السيبرانية الضارة. وتُحدِّد المراحل التي تُمكّن المهاجمين من التحكم بهدفهم وتنفيذ أغراضهم بالنهاية. ويعدّ فهم سلسلة الهجوم السيبراني جزءًا أساسيًا من عملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR). فمن خلال فهم تلك السلسلة يُمكن للمسؤولين عن حماية الشبكات وأمنها تحديد أنماط الهجوم، والتعرف على التقنيات المعروفة التي يستخدمها المهاجمون والاستجابة وفقًا لذلك. وتتكون مراحل سلسلة الهجوم السيبراني من التالي:

المرحلة الأولى، الاستطلاع (Reconnaissance)

يُحدّد المهاجمون الأهداف ويستكشفون نقاط الضعف لاستغلالها أثناء الاستطلاع. وقد تتضمن هذه العملية جمع بيانات الاعتماد والوصول. وجمع المعلومات مثل: عناوين البريد الإلكتروني. وتعرّفات المُستخدمين. والمواقع. ومعلومات التطبيقات. والبرامج. ونظام التشغيل. وبالطبع كلما ازداد كمّ المعلومات التي يتم جمعها كلما أدى إلى المزيد من الهجمات الناجحة.

المرحلة الثانية: التسليح (Weaponization)

يُشحن المهاجم تلقائيًا للهجوم أثناء التسليح (على سبيل المثال: البرمجيات الضارة. وبرمجيات الفدية. والفيروسات. والديدان) الاستغلال لغرة معروفة. وقد يقوم المهاجم أيضًا بإعداد أبواب خلفية للوصول المستمر في حالة تمّرت عملية الدخول بالشكل المخطط له.

86

- وضّح لهم التحديات الرئيسة للتحليل الجنائي الرقمي والاستجابة للحوادث مستعينًا بجدول (2.6).

التوثيق (Documentation):
يجب توثيق عملية التحليل الجنائي الرقمي بأكملها، بما في ذلك الخطوات المتخذة والأدوات المُستخدَمة والاستنتاجات التي تم التوصل إليها. ويضمن التوثيق التفصيلي إمكانية مراجعة التحليل الجنائي وتكراره ونقضه إذا لزم الأمر حسب التزام المُحقّق بأفضل الممارسات والمعايير الصناعية.

الإبلاغ (Reporting):
يُعد عملية التحليل الجنائي الرقمي تُقدَّم الفِرَق الأدلة والنتائج التي تم التوصل إليها. وعادةً ما تُوضّح هذه الخطوة الأخيرة منهجية التحليل والإجراءات المتبعة أثناء التحقيق، مما يضمن تقديم المعلومات بوضوح ودقة للمزيد من المراجعة أو الإجراءات القانونية المحتملة.

عملية الاستجابة للحوادث Incident Response (IR) Process

تمُرّ عملية الاستجابة للحوادث النموذجية بالخطوات التالية:

تحديد النطاق (Scoping):
يكون الهدف في هذه المرحلة تقييم شدة الحادث ونطاقه واتساعه وتحديد جميع مؤشرات الاختراق (Indicators of Compromise – IoC)، كما تساعد هذه الخطوة في تحديد نطاق الهجوم وتحديد أولويات إجراءات الاستجابة وفقًا لذلك.

التحقيق (Investigation):
يتضمّن ذلك استخدام أنظمة متقدمة والمعلومات الاستباقية لاكتشاف التهديدات وجمع الأدلة وتوفير معلومات متعمّقة حول الحادث، وهي خطوة حاسمة في فهم طبيعة الهجوم وجمع البيانات الأساسية للمزيد من التحليل.

التأمين (Securing):
تبقى المؤسسات بحاجة إلى مراقبة صحة أنظمتها الإلكترونية باستمرار حتى بعد معالجة التهديدات. وغالبًا ما تتضمّن هذه المرحلة احتواء التهديدات النشطة التي تم تحديدها أثناء التحقيق واستئصالها، وتلي أي ثغرات أمنية معروفة تلك الهجمات المستغلة.

الدعم والإبلاغ (Support and Reporting):
تختتم مرحلة الدعم والإبلاغ كل حادث أمني بتقديم خطة مفصّلة للدعم المستمر، وبتقديم التقارير المخصصة. وقد يقوم مزود خدمة التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) بتخصيص المُنشأة وتقديم نصيحة اختصاصية بشأن الخطوات التالية لتعزيز التدابير الأمنيّة وضمان الاستعداد للحوادث المستقبلية المحتملة.

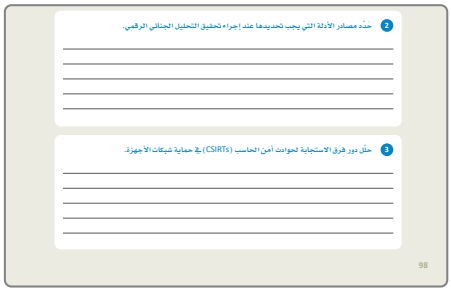
التحوّل (Transformation):
أخيرًا، تتضمّن مرحلة التحوّل من فِرَق التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) تحديد الثغرات في الوضع الأمني للمؤسسة، وتقديم المشورة بشأن تعزيز ثقافة ضعف النظام والحدّ منها، كما تهدف هذه المرحلة إلى تحسين الوضع الأمني للمؤسسة وزيادة صمودها ضد التهديدات السيبرانية المستقبلية.

تحديات التحليل الجنائي الرقمي والاستجابة للحوادث
Digital Forensics and Incident Response Challenges

تزداد التحديات التي يواجهها التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) مع تقدُّم أنظمة الحاسب، وتزداد الهفوات أمام الخبراء في هذا المجال. ويوضّح الجدول 2.6 التحديات الرئيسة التي تواجه التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR).

89

- بيّن للطلبة أهم ممارسات التحليل الجنائي الرقمي والاستجابة للحوادث.
- وجّههم لحل التمرينات الثاني والثالث والرابع والخامس؛ للتحقق من فهمهم لعمليات التحليل الجنائي الرقمي والاستجابة للحوادث.
- اشرح لهم مفهوم **الأمن بدرجة صفر من الثقة** (Zero – Trust Security)، ثم وضّح المبادئ الرئيسة لتنفيذ نموذج الأمن بدرجة صفر من الثقة.
- انتقل بعد ذلك لشرح دور متصفحات الويب في تخزين ملفات السجل، ثم وضّح لهم فائدة استخدام **متصفح دي بي** (DB Browser).
- اشرح لهم كيفية فتح **متصفح دي بي** (DB Browser)، وتحميل ملف السجل.



2 حدّد مصادر الأدلة التي يجب تحديدها عند إجراء تحقيق التحليل الجنائي الرقمي.

3 حلّل دور فرق الاستجابة لحوادث أمن الحاسب (CSIRTs) في حماية شبكات الأجهزة.

98

4 صِف خطوات عملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) النموذجية.

5 صِف التحديات الرئيسة المرتبطة بالتحليل الجنائي الرقمي والاستجابة للحوادث.

99

وزارة التعليم
Ministry of Education
2023 - 1445

- اشرح للطلبة الدور المهم الذي يؤديه جدول محددات موقع الموارد الموحد، ثم وضّح دلالات البيانات الواردة فيه.
- اشرح لهم كيفية قراءة ختم الوقت، ووضّح كيفية استبدال ختم الوقت بتاريخ الإدخال.
- اشرح لهم جدول مصطلحات البحث عن الكلمات الرئيسة، وبيّن أهميته في تحقيقات التحليل الجنائي للأمن السيبراني.
- استمر في الشرح، ووضّح لهم جدول التنزيلات، وبيّن لهم كيفية قراءة البيانات الوصفية المرتبطة بالملفات التي يتم تنزيلها.
- اشرح لهم بعد ذلك جدول تسجيلات الدخول، ثم بيّن الحقول المهمة فيه التي توفر رؤى حول بيانات اعتماد المُستخدِم والبيانات الوصفية.
- في الختام يمكنك توجيه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.

جدول مُحدّدات موقع الموارد المُوحّد The Uniform Resource Locators (URLs) Table

يؤدي جدول عناوين محددات موقع الموارد المُوحد (URLs) دورًا مهمًا في التحقيق. في أنشطة تصفح المُستخدم وتحليلها عند إجراء التحليل الجنائي للأمن السيبراني. ويحتوي هذا الجدول الموجود في سجل متصفح كروم على معلومات قيمة حول عناوين الويب التي زارها المُستخدم أثناء جلسات التصفح. حيث يُمكن للمُحقّقين معرفة مواقع الويب التي تم الوصول إليها بدقة، وتتبّع سلوك المُستخدم. والكشف عن الأدلة الحاسمة المتعلقة بالجرائم الإلكترونية من خلال فحص البيانات المُخزنة في جدول العناوين.

يتكون جدول عناوين مُحدّدات موقع الموارد المُوحّد (URLs) من عدة أعمدة رئيسة توفّر تفاصيل محدّدة حول كل عنوان URL تمت زيارته. فيما يلي، سنستكشف هذه الأعمدة ونتعرف على أهميتها في مجال التحليل الجنائي للأمن السيبراني:

مُحدّد موقع الموارد المُوحّد (url):

يُخزّن عمود مُحدّد موقع الموارد المُوحّد (url) عناوين الويب المحدّدة لمواقع الويب التي تمت زيارتها. حيث يسمح تحليل هذه العناوين للمُحقّقين بتحديد صفحات الويب التي تم الوصول إليها، واسترداد المعلومات الهامة المتعلقة بنشاط معيّن عبر الإنترنت.

العنوان (title):

يحتوي عمود العنوان (title) على عناوين أو أسماء صفحات الويب التي تمت زيارتها. وتُقدّم هذه المعلومات سياقًا إضافيًا وتساعد المُحقّقين على فهم محتوى المواقع التي تم الوصول إليها والغرض منها. كما يُمكن أن يوفّر تحليل العناوين معلومات مهمة حول اهتمامات المُستخدم وعاداته التصفح والمجالات التي يجب تركيز التحقيق حولها.

عداد الزيارة (visit_count):

يُسجّل عمود عداد الزيارة (visit_count) عدد المرات التي زار فيها المُستخدم عنوان URL محدّد. ويسمح هذا العداد للمُحقّقين بتحديد وتيرة ومستوى استخدام المُستخدم لموقع ويب معيّن. كما يساعد هذا التحليل في تحديد الموارد التي تم الوصول إليها بشكل متكرر. وتحديد أولويات جهود التحقيق. وتحديد أنماط أو اتجاهات سلوك المُستخدم.

وقت آخر زيارة (last_visit_time):

يُوفّر عمود وقت آخر زيارة (last_visit_time) ختم الوقت أو تاريخ آخر مرة تمت زيارة لعنوان URL محدّد ووقتها. وتُمكّن هذه المعلومات المُحقّقين من إنشاء جداول زمنية وتتبّع التسلسل الزمني لأنشطة المُستخدم. وربما ربط زيارات موقع الويب بأحداث أو إجراءات أخرى.

94

قراءة ختم الوقت Reading a Timestamp

ختم الوقت (Timestamp) هو قيمة رقمية تمثّل نقطة زمنية محدّدة. ويُستخدم بشكل شائع في قواعد البيانات وأنظمة الحاسب لتسجيل وتتبّع الأحداث أو إنشاء البيانات وتعديلها. وغالبًا ما يتم تخزين أختام الوقت على هيئة رقم يمثّل الثواني أو المِلّي ثانية منذ نقطة مرجعية محدّدة تُعرف باسم الحقبة (Epoch).

يُمكنك استخدام البرنامج النصي التالي في علامة تبويب تنفيذ SQL (Execute SQL) في متصفح دي بي (DB Browser) لعرض تاريخ الإدخال عن طريق استبدال ختم الوقت (Timestamp) بالقيمة التي تريد عرضها:

```
SELECT datetime (timestamp/1000000 +
                (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime')
```

لقراءة ختم الوقت (Timestamp):

- اضغط على علامة تبويب Execute SQL (تنفيذ SQL).
- أدخل البرنامج النصي مع ختم الوقت الذي ترغب في ترجمته في الحقل أعلاه.
- اضغط على زر Run (تشغيل) لتشغيل البرنامج النصي.

شكل 2.26: قراءة ختم الوقت (Timestamp)

95

تمرينات

1

حدد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُركّز التحليل الجنائي الرقمي على استعادة الملفات المحذوفة وفك تشفير البيانات.		
2. التحليل الجنائي الرقمي والاستجابة للحوادث عمليات مختلفة.		
3. يُستخدم التحليل الجنائي الرقمي في الإجراءات القانونية فقط.		
4. تتضمن الاستجابة للحوادث جمع البيانات وتحليلها لتحديد تفاصيل أي حادث أمن سيبراني.		
5. تؤدي فِرَق الاستجابة لحوادث أمن الحاسب (CSIRTs) دورًا أساسيًا في الأمن السيبراني.		
6. لا تُعدّ مراجعة ما بعد الحادث ضرورية لعملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR).		
7. يشمل جمع الأدلة الجنائية تجميع البيانات من مصدر واحد فقط.		
8. يتطابق التحليل الجنائي للذاكرة مع التحليل الجنائي لنظام الملفات.		

98

يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُركِّز التحليل الجنائي الرقمي على استعادة الملفات المحذوفة وفَك تشفير البيانات.	✓	
2. التحليل الجنائي الرقمي والاستجابة للحوادث عمليات مختلفة.	✓	
3. يُستخدم التحليل الجنائي الرقمي في الإجراءات القانونية فقط. يتم استخدامه في التحقيقات الداخلية أيضًا.		✓
4. تتضمن الاستجابة للحوادث جَمع البيانات وتحليلها لتحديد تفاصيل أي حادث أمن سيبراني. هذه هي عملية التحليل الجنائي الرقمي.		✓
5. تؤدّي فِرَق الاستجابة لحوادث أمن الحاسب (CSIRTs) دورًا أساسيًا في الأمن السيبراني.	✓	
6. لا تُعدُّ مراجعة ما بعد الحادث ضرورية لعملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR). إنها جزء مهم من عملية التحليل الجنائي الرقمي والاستجابة للحوادث(DFIR).		✓
7. يَشمل جَمع الأدلة الجنائية تجميع البيانات من مَصدر واحد فقط. يشمل تجميع البيانات من أكبر قدر ممكن من المصادر.		✓
8. يتطابق التَحليل الجنائي للذاكرة مع التَحليل الجنائي لنظام الملفات. هما طريقتان مختلفتان.		✓

2 حَدِّد مصادر الأدلة التي يجب تحديدها عند إجراء تحقيق التحليل الجنائي الرقمي.

- التحليل الجنائي لنظام الملفات: هو التحقيق في أنظمة ملفات النقطة الطرفية لتحديد مؤشرات الاختراق الأمني أو استغلال الثغرات.
- التحليل الجنائي للذاكرة: هو فحص ذاكرة النظام للكشف عن أي مؤشرات لوجود الثغرات التي قد لا تكون موجودة في أنظمة الملفات.
- التحليل الجنائي للشبكة: هو تحليل نشاط الشبكة مثل: رسائل البريد الإلكتروني، والرسائل، وسجل التصفح للتعرُّف على الهجوم وفَهم أساليبه وتحديد نطاق الحادث.
- تحليل السجلات: مراجعة وتفسير سجلات النشاط لاكتشاف الأحداث غير العادية أو السلوك المشبوه الذي قد يشير إلى وقوع حادث أمني.

3 حلِّل دور فِرَق الاستجابة لحوادث أمن الحاسب (CSIRTs) في حماية شبكات الأجهزة.

فرق الاستجابة لحوادث أمن الحاسب هي مجموعات متخصصة من المهنيين التقنيين الذين يقومون بالتحقيق في حوادث الأمن الرقمي وتحليلها والاستجابة لها. إنهم يلعبون دورًا حاسمًا في حماية شبكات الحاسب واستعادتها بعد تحديد المشكلات الأمنيّة.

يمكن تقديم إجابات إضافية من قبل الطلبة

4 صِف خطوات عملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) النموذجية.

- جَمع الأدلة الجنائية: يتضمن ذلك عملية جمع البيانات وفحصها وتحليلها من مصادر مختلفة مثل: الشبكات، والتطبيقات، ومخازن البيانات، والنقاط الطرفية سواء في مراكز البيانات داخل الشركات أو الخدمات السحابية.
- سلسلة الحيازة: إجراء يتم به الاستمرار في جمع الأدلة الجنائية من خلال تَتَبُّع رحلة الأدلة من الجمع إلى التحليل، كما يتضمن توثيق تفاعل كل فرد مع الأدلة، وتاريخ الجمع أو النقل ووقته، وسبب النقل.
- التحقيق في السبب الجذري: يتم في هذه الخطوة تحديد ما إذا كانت المؤسسة هدفًا أساسيًا للخَرق، وتحديد السبب الجذري للحادث، ونطاقه، والجدول الزمني لحدوثه وتأثيره.
- الإخطار والإبلاغ: تقوم المؤسسات بإخطار السلطات المختصة بخصوص الانتهاكات أو التهديدات الأمنيّة اعتمادًا على التزامات الامتثال الخاصة بها.
- مراجعة ما بعد الحادث: قد تتطلب هذه المرحلة من المؤسسة التفاوض مع المهاجِمين، والتواصل مع أصحاب المصلحة والعملاء والصحافة، وتنفيذ تغييرات على الأنظمة والعمليات لمعالجة الثغرات الأمنيّة اعتمادًا على طبيعة الحادث.

5 صِف التحديات الرئيسة المرتبطة بالتحليل الجنائي الرقمي والاستجابة للحوادث.

التحديات الرئيسة للتحليل الجنائي الرقمي والاستجابة للحوادث	
التحدي	الوصف
التحليل الجنائي الرقمي	
تعدد مصادر الأدلة	لم تَعُدْ إمكانية إعادة إنشاء الأدلة الرقمية تعتمد على موقع أو خادم أو شبكة واحدة؛ بل أصبحت تنتشر خلال العديد من المواقع المادية والافتراضية، ونتيجة لذلك تتطلب التحاليل الجنائية الرقمية مزيدًا من الخبرة والأدوات والوقت لجمع التهديدات والتحقيق فيها بدقة وكفاءة.
الوتيرة المتسارعة للتقنية	تتطوَّر الأجهزة الرقمية وتطبيقات البرمجيات وأنظمة التشغيل وتتوسع باستمرار، ونظرًا لمعدل التغيير السريع يتعين على خبراء التحليل الجنائي الرقمي أن يكونوا قادرين على إدارة الأدلة الرقمية في مجموعة متنوعة من إصدارات التطبيقات وتنسيقات الملفات.
الاستجابة للحوادث	
تزايد البيانات ونُدْرَة الدعم	تواجه المؤسسات عددًا متزايدًا من التنبيهات الأمنيّة، ومع ذلك، فهي على الأغلب لا تمتلك الخبرة الكافية في مجال الأمن السيبراني اللازمة لمعالجة حجم المعلومات وحجم التهديدات، حيث تعتمد المؤسسات على الخبراء الخارجيين في التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) لسد فجوة المهارات، والحصول على الدعم أثناء التهديدات الحرجة.
تَوسُّع نطاق الهجوم	يجعل تَوسُّع نطاق الهجوم لأنظمة الحوسبة والبرمجيات الحديثة عملية الحصول على ملخص دقيق للشبكة أكثر صعوبة، ويزيد من مخاطر التهيئة الخاطئة وأخطاء المُستخدِمين.

يمكن تقديم إجابات إضافية من قبل الطلبة

6 باستخدام متصفح الويب الذي يحتوي على كَم كبير من بيانات الأنشطة، حلِّل النتائج من جدول عناوين URL، وحاوِل تحديد ما إذا كانت هناك أنماطٌ معيَّنة يتبعها المُستخدِم في نشاط تصفح الويب الخاص به.

تلميح: شجّع الطلبة على اكتشاف نمط أو سلوك متكرر في المواقع التي يزورونها وأوقات زيارتها، وعددها. على سبيل المثال: سيكون النمط النموذجي خلال اليوم هو التحقق من المواقع الإخبارية كل صباح، ثم التحقق من حسابات وسائل التواصل الاجتماعي ما بين 30 إلى 45 دقيقة، وزيارة المنصات الإلكترونية لأداء واجباتهم المدرسية، ثم زيارة مواقع البث في فترة ما بعد الظهر والمساء للترفيه.

7 باستخدام طبيعة البيانات نفسها من التمارين السابقة، قَيِّم البيانات من جدول تسجيلات الدخول (Logins) واسرد المواقع التي أدخل فيها المُستخدِم بيانات اعتماده، ثم صنِّف هذه المواقع على أنها آمنة أو غير آمنة.

تلميح: وجّه الطلبة لملاحظة أن المواقع غير الآمنة تشتمل على الخصائص التالية:

- ليس لديها تشفير **طبقة المنافذ الآمنة**(SSL).
- تبدو سيئة التصميم.
- ليس لديها وظيفة **تسجيل الدخول الموحَّد** (SSO).
- لا تتطلب إنشاء كلمة مرور قوية.

المشروع

أهداف المشروع:

- تحديد طرائق العثور على جميع الأجهزة المصابة من قِبل فريق الاستجابة للحوادث، ومعرفة كيفية التصدي للفيروسات في الأجهزة.
- شرح خطوات منع انتشار الفيروس عبر الأجهزة المصابة، وكيفية التعامل معها بعد الإصابة.
- تحليل الكيفية التي يجب التعامل بها مع الأجهزة المصابة التي تحتوي على معلومات حساسة.
- وصف التدابير التي يحتاج فريق الاستجابة للحوادث تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.
- إنشاء عرض تقديمي لتحليل سيناريو الخطوات السابقة.

- قسّم الطلبة لمجموعات متكافئة، واطلب منهم تخطيط المشروع قبل البدء فيه.
- وجّههم للرجوع للمفاهيم النظرية والخطوات العملية في الوحدة عند الحاجة.
- ضع معايير مناسبة لتقييم أعمال الطلبة في المشروع، وتأكّد من فهم لمتطلبات المشروع.
- يمكنك الاسترشاد بمعايير تقييم المشاريع الواردة في الدليل العام.
- قيّمهم وَفْقَ معايير التقييم، وقدّم لهم التغذية الراجعة للوصول لأفضل نتيجة.
- أخيرًا، حدِّد موعد تسليم المشروع ومناقشة أعمال المجموعات.

سُلّم التقدير

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
المعرفة: تحديد طرائق العثور على جميع الأجهزة المصابة من قِبل فريق الاستجابة للحوادث، ومعرفة كيفية التصدي للفيروسات في الأجهزة	تحديد طريقة للعثور على جميع الأجهزة المصابة، وعدم تحديد طرائق التصدي للفيروسات في الأجهزة.	تحديد طريقتين للعثور على جميع الأجهزة المصابة، وعدم تحديد طرائق التصدي للفيروسات في الأجهزة.	تحديد ثلاث طرائق للعثور على جميع الأجهزة المصابة، وعدم تحديد طرائق التصدي للفيروسات في الأجهزة.	تحديد أربع طرائق للعثور على جميع الأجهزة المصابة، وتحديد طرائق التصدي للفيروسات في الأجهزة.
المعرفة: شرح خطوات منع انتشار الفيروس عبر الأجهزة المصابة، وكيفية التعامل معها بعد الإصابة	تحديد بعض خطوات منع انتشار الفيروس عبر الأجهزة المصابة، وعدم ذِكر كيفية التعامل معها بعد الإصابة.	تحديد أغلب خطوات منع انتشار الفيروس عبر الأجهزة المصابة، وعدم ذِكر كيفية التعامل معها بعد الإصابة.	تحديد جميع خطوات منع انتشار الفيروس عبر الأجهزة المصابة، وعدم ذِكر كيفية التعامل معها بعد الإصابة.	تحديد جميع خطوات منع انتشار الفيروس عبر الأجهزة المصابة، مع ذِكر كيفية التعامل معها بعد الإصابة.
المعرفة:تحليل الكيفية التي يجب التعامل بها مع الأجهزة المصابة التي تحتوي على معلومات حساسة	لم يحدِّد الكيفية التي يجب التعامل بها مع الأجهزة المصابة التي تحتوي على معلومات حساسة.	حدَّدَ نقطتين من للكيفية التي يجب التعامل بها مع الأجهزة المصابة التي تحتوي على معلومات حساسة.	حدَّدَ ثلاث نقاط من للكيفية التي يجب التعامل بها مع الأجهزة المصابة التي تحتوي على معلومات حساسة.	حدَّدَ أربع نقاط فأكثر للكيفية التي يجب التعامل بها مع الأجهزة المصابة التي تحتوي على معلومات حساسة.
المعرفة: وصف التدابير التي يحتاج فريق الاستجابة للحوادث تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها	لم يحدِّد أيًّا من التدابير التي يحتاج فريق الاستجابة للحوادث تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.	حدَّدَ واحدًا من التدابير التي يحتاج فريق الاستجابة للحوادث تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.	حدَّدَ اثنين من التدابير التي يحتاج فريق الاستجابة للحوادث تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.	حدَّدَ ثلاثة فأكثر من التدابير التي يحتاج فريق الاستجابة للحوادث تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
المهارة: إنشاء عرض تقديمي لتحليل سيناريو الخطوات السابقة	أنشَأ عرضًا تقديميًا يتضمن فقرة حول تحليل سيناريو الخطوات السابقة.	أنشَأ عرضًا تقديميًا يتضمن فقرتين حول تحليل سيناريو الخطوات السابقة.	أنشأ عرضًا تقديميًا يتضمن ثلاث فقرات حول تحليل سيناريو الخطوات السابقة.	أنشَأ عرضًا تقديميًا يتضمن أربع فقرات حول تحليل سيناريو الخطوات السابقة.
التفكير الناقد	لا يظهر فهمًا للمشكلة أو أهداف المهمة، وينظر لها بشكل سطحي، ويقبل المعلومات من غير تقييم لمصداقيتها.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد بعض الجوانب لما يجب معرفته وطرح الأسئلة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها. يدرك أهمية مصداقية المعلومات لكن لا يتخذ إجراءات للتأكد من ذلك.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد بعض الجوانب لما يجب معرفته وطرح الأسئلة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها. يقيم الحجج من خلال تقييم الأدلة الداعمة لها.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد ما يجب معرفته، وطرح الأسئلة حسب الحاجة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها ويقيم مصداقيتها، ويميز بين الحقيقة والرأي. يقيم الحجج من خلال تقييم الأدلة الداعمة لها. ويبرر سبب القبول أو الرفض وفق معايير محددة وواضحة.
الإبداع	يولد عددًا محدودًا من الأفكار التي لا ترتبط بالمشكلة أو أهداف المهمة. المنتج نسخة لأمثلة أو إجابات نموذجية سابقة.	يولد عددًا محدودًا من الأفكار التي قد ترتبط بالمشكلة أو أهداف المهمة. المنتج نسخة لأمثلة أو إجابات نموذجية سابقة أو يتضمن توظيف أكثر من طريقة معروفة مسبقًا.	يولد عددًا محدودًا من الأفكار ذات الصلة المباشرة بالمشكلة أو أهداف المهمة. يتضمن المنتج بعض الجوانب المبتكرة، ويتصف بالفائدة العملية.	يولد عددًا من الأفكار ذات الصلة المباشرة بالمشكلة أو أهداف المهمة، ويستخدمها لتطوير حل للمشكلة أو تحقيق أهداف المهمة. يتصف المنتج بالأصالة والابتكار والفائدة العملية.

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
العمل مع الآخرين	غير مستعد للعمل والتعاون مع الآخرين، لا يشارك في حل المشكلات أو طرح الأسئلة أو المناقشات.	يقوم ببعض المهام في المشروع ويتعاون مع الفريق، ولكن قد لا يساهم بنشاط في حل المشكلات أو طرح الأسئلة أو المناقشات.	يقوم بأداء مهامه في المشروع، يتعاون مع الفريق ويساهم في حل المشكلات وطرح الأسئلة والمناقشات، ويعطي ملاحظات لمساعدة الفريق.	يقوم بأداء مهامه في المشروع ويكملها في الوقت المحدد، يتعاون مع الفريق ويساهم في حل المشكلات وطرح الأسئلة والمناقشات بناءً على الأدلة، ويعطي ملاحظات بناءة لمساعدة الفريق وتحسين العمل.
العرض	لا يفي بمتطلبات ما يجب تضمينه في العرض، لا يقدم معلومات واضحة، يستخدم أسلوبًا غير مناسب لأهداف المهمة والجمهور.	يلبي بعض المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة)، يقدم بعض المعلومات الواضحة، ويستخدم أسلوبًا مناسبًا نوعًا ما لأهداف المهمة والجمهور.	يفي بمعظم المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة واضحة)، يقدم المعلومات بوضوح، ويستخدم أسلوبًا مناسبًا لأهداف المهمة والجمهور.	يفي بجميع المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة واضحة ومثيرة للاهتمام، ينظم الوقت بشكل جيد)، يقدم جميع المعلومات بوضوح ودقة وفق تسلسل منطقي، ويستخدم أسلوبًا مناسبًا لأهداف المهمة والجمهور.

تلميح: **محكات المعرفة والمهارات تعتبر أساسية لاستيفاء أهداف المشروع بينما يمكن للمعلّم استخدام محكات (التفكير الناقد / الإبداع / العمل مع الآخرين / العرض) حسب ما يراه مناسب.**

الوحدة الثالثة

مواضيع متقدِّمة في الأمن السيبراني

وصف الوحدة

عزيزي المعلّم

الغرض العام من الوحدة هو أن يتمكن الطلبة من تحديد النقاط الرئيسة بالتشريعات الموحدة للأمن السيبراني، ويصنفوا قوانين الأمن السيبراني الرئيسة وضوابطه في المملكة العربية السعودية والدول الأخرى، ويفسروا المقصود بالتشفير واستخداماته، ويميزوا بين أنواع التشفير وأنواع التهديدات المحتملة من المتسللين، وينفذوا خوارزميات التشفير باستخدام لغة البايثون ، ويحللوا كيفية حماية أنظمة الأمن السيبراني للتطبيقات المُنشأة باستخدام التقنيات الناشئة.

أهداف التعلُّم

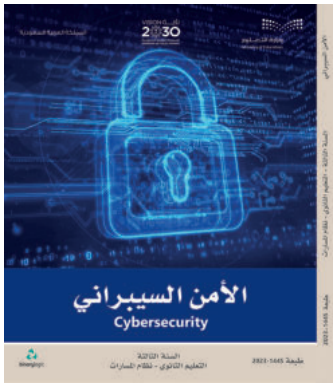
- تحديد النقاط الرئيسة للتشريعات الموحدة للأمن السيبراني.
- تصنيف قوانين الأمن السيبراني الرئيسة وضوابطه في المملكة العربية السعودية والدول الأخرى.
- تفسير المقصود بالتشفير واستخداماته.
- التمييز بين أنواع التشفير وأنواع التهديدات المحتملة من المُتسلِّلين.
- تنفيذ خوارزميات التشفير باستخدام لغة البايثون.
- تحليل كيفية حماية أنظمة الأمن السيبراني للتطبيقات المُنشأة باستخدام التقنيات الناشئة.

وزارة التعليم
Ministry of Education
2023 - 1445

الدروس	
الوحدة الثالثة : مواضيع متقدِّمة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: تشريعات وقوانين الأمن السيبراني	1
الدرس الثاني: التشفير في الأمن السيبراني	3
الدرس الثالث: الأمن السيبراني والتقنيات الناشئة	3
المشروع	3
إجمالي عدد حصص الوحدة الثالثة	**10**

المصادر والملفات والأدوات والأجهزة المطلوبة

المصادر



كتاب الأمن السيبراني

التعليم الثانوي – نظام المسارات

السنة الثالثة

الملفات الرقمية

يُمكنك الوصول للحلول أو الملفات النهائية للتمرينات التي يمكن استخدامها على منصة "عين" الإثرائية، وهي:

- مجلد G12.CYB.S3.U3

الأدوات والأجهزة

- **البايثون** (Python)

تشريعات وقوانين الأمن السيبراني

وصف الدرس

الهدف العام من الدرس هو التعرف على أهمية تشريعات الأمن السيبراني وقوانينه بشكل عام، وقوانين الأمن السيبراني وتشريعاته في المملكة العربية السعودية، بالإضافة لمعرفة القوانين والضوابط الدولية للأمن السيبراني.

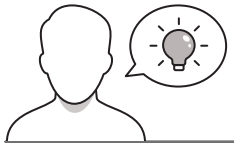
أهداف التعلُّم

- معرفة أهمية تشريعات الأمن السيبراني وقوانينه.
- معرفة قوانين الأمن السيبراني وتشريعاته في المملكة العربية السعودية.
- معرفة القوانين والضوابط الدولية للأمن السيبراني.

الدرس الأول	
الوحدة الثالثة: مواضيع متقدِّمة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الأول: تشريعات وقوانين الأمن السيبراني	1

نقاط مهمَّة

- قد يظن بعض الطلبة أن تطبيق قوانين الأمن السيبراني وتشريعاته مقتصر على حماية المنشآت فقط من التهديدات السيبرانية، بيّن لهم أنها تشمل أيضًا حماية الأفراد منها.
- قد يظن بعض الطلبة أن بعض الممارسات ليس لها علاقة بالجرائم الإلكترونية، وضّح لهم أن هناك ممارسات تندرج تحت الجرائم الإلكترونية مثل: انتحال الشخصية، وغيرها.

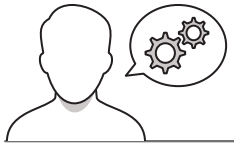


التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- لماذا تلجأ الجهات والمنظمات لسَنّ التشريعات والقوانين للأمن السيبراني؟
- ما الجهات الحكومية المسؤولة عن قوانين الأمن السيبراني في المملكة العربية السعودية؟
- ما المقصود بالجرائم الإلكترونية؟



خطوات تنفيذ الدرس

> في البداية ناقِش الطلبة حول الحاجة لسَنّ تشريعات وقوانين الأمن السيبراني.

> اشرح لهم أهم اعتبارات الاستخدام الصحيح للتشريعات والقوانين المُنظِّمة لمجال الأمن السيبراني.

> اطلب منهم حل التمرين الثاني؛ للتحقق من فهمهم لأهمية التشريعات والقوانين للأمن السيبراني.

> اشرح لهم قوانين الأمن السيبراني وتشريعاته في المملكة العربية السعودية.

> استخدم الشكل (3.1) لشرح المكونات الأساسية **للضوابط الأساسية للأمن السيبراني** (ECC).

> اشرح لهم المكونات الأساسية والفرعية **لضوابط الأمن السيبراني للبيانات** (DCC).

> يمكنك توجيه الطلبة لحل التمرين الثالث؛ للتحقق من فهمهم لضوابط الأمن السيبراني للبيانات.

الردع والملاحقة القضائية (Deterrence and Prosecution):
تُحدّد قوانين الأمن السيبراني مختلف الجرائم الإلكترونية وتُصنّفها حسب طبيعتها، مما يسمح لجهات تنفيذ القانون بملاحقة الجُناة ومقاضاتهم. كما تعمل هذه القوانين كرادع ضد الأنشطة السيبرانية الضارة، وتضمن محاسبة مُرتكبي الجرائم السيبرانية على أفعالهم.

التعاون الدولي (International Cooperation):
تُبرز الحاجة إلى التعاون الدولي لمكافحة الجرائم الإلكترونية نظرًا للنطاق الواسع والمادي للتهديدات والهجمات السيبرانية. وتُسهم تشريعات الأمن السيبراني وقوانينه في تعزيز التعاون بين الدول، مما يتيح تبادل المعلومات الاستخبارية وأفضل الممارسات في مجال معالجة التهديدات السيبرانية العالمية.

قوانين الأمن السيبراني وتشريعاته في المملكة العربية السعودية
Cybersecurity Laws and Regulations in KSA

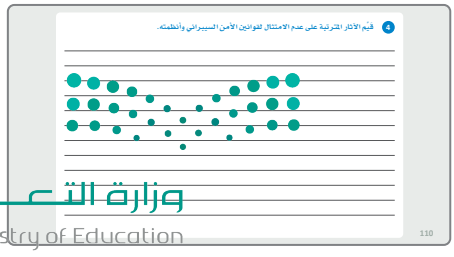
ضوابط الأمن السيبراني Cybersecurity Controls

نشرت الهيئة الوطنية للأمن السيبراني (NCA) في المملكة العربية السعودية العديد من ضوابط الأمن السيبراني التي يجب على الكيانات العامة والخاصة العاملة في المملكة العربية السعودية الالتزام بها، وتلك الضوابط هي تدابير تقنية وغير تقنية مُصممة لحماية أنظمة الحاسب والشبكات والبيانات من الوصول غير المُصرّح به، أو سوء الاستخدام، أو التعديل، أو الإتلاف، أو تعطيل الوصول للبيانات والأنظمة. وفيما يلي نظرة عامة على هذه الضوابط:

الضوابط الأساسية للأمن السيبراني (Essential Cybersecurity Controls - ECC):
يُعدُّ توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني الهدف الرئيس لهذه المتطلبات التي صُمّمت بناءً على أفضل الممارسات والمعايير لحماية الأصول المعلوماتية للجهات من التهديدات الداخلية والخارجية وتقليل المخاطر السيبرانية. كما تتناول هذه الضوابط جوانب مختلفة من الأمن السيبراني، بما في ذلك إدارة الأصول وعمليات الدخول والصلاحيات، وإدارة حوادث وتهديدات الأمن السيبراني، والتوعية والتدريب بالأمن السيبراني. وتُعدّ هذه الضوابط ملزمة على جميع الجهات الحكومية في المملكة العربية السعودية، بما في ذلك الوزارات والهيئات والمؤسسات وغيرها، والجهات والشركات التابعة لها، وجهات القطاع الخاص التي لديها بُنى تحتية وطنية حسّاسة (Critical National Infrastructures - CNIs) أو تعمل على تشغيلها أو استضافتها؛ وذلك لضمان حماية أنظمة المعلومات الخاصة بها.

شكل 3.1: المكونات الأساسية للضوابط (ECC - 1: 2018)

104



4 قيم الآثار المترتبة على عدم الامتثال للقوانين الأمن السيبراني وأنظمته.

110

- اشرح لهم ضوابط الأمن السيبراني للحوسبة السحابية وللعمل عن بُعد، وللأنظمة الحسَّاسة، وللأنظمة التشغيلية.
- انتقل لتوضيح أنظمة الجرائم الإلكترونية (Cybercrime Regulation) في المملكة العربية السعودية، وبيّن أهميتها في حماية خصوصية وأمن الأفراد والمنشآت.
- وضّح للطلبة **قانون حماية البيانات الشخصية** (PDPL)، ودوره في حماية حقوق الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قِبَل الكيانات في المملكة وخارجها.
- استمر في الشرح بتوضيح قانون مكافحة جرائم المعلوماتية، ومثّل لأنشطة الجرائم الإلكترونية مثل: القرصنة، والاحتيال عبر الإنترنت، وغيرها.
- يمكنك توجيه الطلبة لحل التمرين الخامس؛ للتحقق من فهمهم لقانون مكافحة الجرائم المعلوماتية في المملكة.

ضوابط الأمن السيبراني للعمل عن بُعد (Telework Cybersecurity Controls):
الغرض من هذه الوثيقة هو رفع جاهزية الجهات للعمل عن بُعد بشكل آمن والتكيف مع تغيرات بيئات وأنظمة العمل عن بُعد، بالإضافة لتعزيز قدرات الأمن السيبراني للجهات للصمود ضد التهديدات السيبرانية عند العمل عن بُعد.

ضوابط الأمن السيبراني للأنظمة الحسَّاسة (Critical Systems Cybersecurity Controls):
تهدف هذه الضوابط إلى تطوير قدرات الحماية والصمود ضد الهجمات السيبرانية، وذلك لتمكين الجهات ذات الأنظمة الحساسة من المحافظة على أصولها المعلوماتية والتقنية تلبية الاحتياجات الأمنية الحالية وتعزيز جاهزية الجهات حيال المخاطر السيبرانية المتزايدة والتي قد ينجم عنها تأثيرات ضارة على المستوى الوطني.

ضوابط الأمن السيبراني للأنظمة التشغيلية (Operational Technology Cybersecurity Controls):
تهدف هذه الضوابط إلى رفع جاهزية الجهات حتى تتمكن من حماية أنظمتها التشغيلية، كما تحدّد الوثيقة الحد الأدنى من متطلبات الأمن السيبراني للأنظمة التشغيلية في المرافق الصناعية الحساسة لدى الجهات الحكومية والخاصة لمنع الوصول غير المُصرَّح به لهذه الأنظمة.

أنظمة الجرائم الإلكترونية Cybercrime Regulation

تم تشريع العديد من القوانين والضوابط في المملكة العربية السعودية لمكافحة الجرائم الإلكترونية وحماية خصوصية وأمن الأفراد والمنشآت، وفيما يلي لمحة عامة حول أبرزها:

قانون حماية البيانات الشخصية (Personal Data Protection Law – PDPL):
تم تشريع **قانون حماية البيانات الشخصية** (PDPL) ولوائحه التنفيذية لحماية خصوصية الأفراد في المملكة العربية السعودية، حيث يعتبر الأساس القانوني لحماية حقوق الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قِبَل جميع الكيانات في المملكة وخارجها لجميع الأفراد في المملكة باستخدام أي وسيلة، بما في ذلك معالجة البيانات الشخصية عبر الإنترنت.

قانون مكافحة جرائم المعلوماتية (Anti-Cyber Crime Law):
قانون مكافحة جرائم المعلوماتية في المملكة العربية السعودية هو مجموعة من القوانين والضوابط التي تُحرِّم مجموعة واسعة من أنشطة الجرائم الإلكترونية. وقد تم سنّ القانون لحماية الأمن القومي للبلاد ومصالحها الاقتصادية من التهديدات السيبرانية، وضمان سلامة المواطنين والمقيمين من الجرائم الإلكترونية.
يُحرِّم قانون مكافحة جرائم المعلوماتية كافة أنشطة الجرائم الإلكترونية مثل: القرصنة، والاحتيال عبر الإنترنت، وانتحال الشخصية، وانتهاك الخصوصية. كما يتضمن أحكامًا لحماية البيانات الشخصية والتحقيق في الجرائم الإلكترونية والملاحقة القضائية لمرتكبيها.
بموجب قانون مكافحة جرائم المعلوماتية تُعدُّ الجريمة الإلكترونية جريمة خطيرة يُعاقب عليها بالغرامة والسجن وعقوبات أخرى. كما يُخوِّل القانون الحكومة باتخاذ تدابير لمنع الوصول إلى مواقع الويب التي تُعدُّ مُتورِّطة في الجرائم الإلكترونية.

106

5 عرّف قانون مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

110

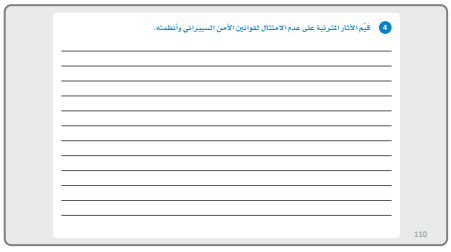
- اشرح للطلبة أبرز القوانين والضوابط الدولية للأمن السيبراني حول العالم.
- يمكن بعدها تقسيم الطلبة لمجموعات متكافئة، واطلب من كل مجموعة الاطلاع على القوانين والضوابط الدولية لعدد من الدول، ثم اطلب منهم تلخيص أبرز تلك القوانين، ثم ناقِشها معهم، وقدّم التغذية الراجعة لهم.
- بنفس المجموعات السابقة اطلب من كل مجموعة حل التمرينين السادس والسابع، للتحقق فهمهم للضوابط الأساسية للأمن السيبراني، والأنظمة العالمية له.

6 ابحث في الإنترنت عن الضوابط الأساسية للأمن السيبراني (ECC)، وأذكر الضوابط الرئيسة لبرنامج التوعية بالأمن السيبراني، والتدريب عليه.

7 قيّم الآثار المترتبة على النظام الأوروبي العام لحماية البيانات (GDPR) على الشركات العاملة عبر الحدود.

111

> في الختام وجِّه الطلبة لحل التمرينين الأول والرابع؛ للتحقق من فهمهم لأهداف الدرس.



يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يَقتصر تطبيق القوانين والضوابط الخاصة بالأمن السيبراني على حماية المنشآت من التهديدات السيبرانية. يتم استخدامها لحماية الأفراد أيضًا.	○	✓
2. يَعمل وجود المعايير القياسية لقوانين الأمن السيبراني وضوابطه على تعزيز مستويات الأمن.	✓	○
3. لا تتحمَّل الحكومات والمؤسسات أي مسؤولية حول أي اختراقات أمن سيبراني. يمكن محاسبتهم أيضًا.	○	✓
4. لا يُعدُّ التعاون الدولي أساسيًا في مكافحة الجريمة الإلكترونية. إنه أمر حتمي لأن الجريمة السيبرانية عالمية بطبيعتها.	○	✓
5. لا تؤثِّر قوانين الأمن السيبراني وضوابطه على ثِقة العملاء في المُنتَجات والخدمات. التنظيم الأفضل يؤدي إلى زيادة ثقة المستهلك.	○	✓
6. تَهدف الهيئة الوطنية للأمن السيبراني (NCA) إلى حماية مصالح المملكة من خلال تعزيز البنيَة التحتيَّة للأمن السيبراني.	✓	○
7. تتناول الضوابط الأساسية للأمن السيبراني (ECC) إدارة هويات الدخول والصلاحيات فقط. يتناول مجموعةً من الجوانب الأخرى بما في ذلك إدارة حوادث وتهديدات الأمن السيبراني، والتوعية والتدريب بالأمن السيبراني.	○	✓
8. يُوفِّر قانون حماية البيانات الشخصية (PDPL) تَدابير لإدارة الأمن السيبراني السحابي. ويتعلق أيضًا بحماية البيانات والخصوصية.	○	✓
9. يُنظِّم قانون نقل التأمين الصحي والمساءلة (HIPPA) عملية الوصول غير المُصرَّح به للبيانات المالية الرقمية. يغطي حماية البيانات الصحية وليس المالية.	○	✓
10. يُغطِّي قانون مكافحة جرائم المعلوماتية السعودي كلًا من أمن الأفراد وأمن المؤسسات.	✓	○

يمكن تقديم إجابات إضافية من قبل الطلبة

2 اشرح فوائد المعايير القياسية لقوانين الأمن السيبراني في الشركات والمؤسسات.

تُوفِّر تشريعات الأمن السيبراني وقوانينه مجموعةً قياسيةً من المعايير وأفضل الممارسات التي يجب على المنشآت اتِّباعُها، مما يُعزِّز مستويات الأمن على مستوى المؤسسات والصناعات المختلفة، كما يُسهِّل وجود المعايير القياسية عملية التعاون بين المؤسسات، ويُوفِّر استراتيجيات استجابة موحَّدة أكثر فعالية للتهديدات السيبرانية.

3 حلِّل فئتين فرعيتين من ضوابط الأمن السيبراني للبيانات.

- ضوابط الأمن السيبراني للعمل عن بُعد: الغرض من هذه الوثيقة هو توجيه المؤسسات لأداء العمل عن بعد بشكل آمِن، والتكيّف مع التغيرات في بيئات وأنظمة العمل عن بُعد عند توفيره.
- ضوابط الأمن السيبراني للأنظمة الحسَّاسة: تقدم هذه الوثيقةُ ضوابطَ محددة لإدارة الأمن السيبراني للأنظمة السحابية للمؤسسات التي تُعَد ذات مهام حساسة وحرجة.

يمكن تقديم إجابات إضافية من قبل الطلبة

4 قَيِّم الآثار المترتبة على عدم الامتثال لقوانين الأمن السيبراني وأنظمته.

تُعدُّ الجريمة الإلكترونية جريمة خطيرة يُعاقب عليها بالغرامة والسجن وعقوبات أخرى، كما يُخوّل القانون الحكومة باتخاذ تدابير لمنع الوصول إلى مواقع الويب التي تُعدُّ مُتورِّطةً في الجرائم الإلكترونية.

5 عَرِّف قانون مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

قانون مكافحة جرائم المعلوماتية في المملكة العربية السعودية هو مجموعة من القوانين والضوابط التي تُجرِّم مجموعة واسعة من أنشطة الجرائم الإلكترونية، ولقد تم سَنُّ القانون لحماية الأمن القومي للبلاد ومصالحها الاقتصادية من التهديدات السيبرانية، وضمان سلامة المواطنين والمقيمين من الجرائم الإلكترونية.

يُجرِّم قانون مكافحة جرائم المعلوماتية كافة أنشطة الجرائم الإلكترونية مثل: القرصنة، والاحتيال عبر الإنترنت، وانتحال الشخصية، وانتهاك الخصوصية، كما يتضمن أحكامًا لحماية البيانات الشخصية والتحقيق في الجرائم الإلكترونية والملاحقة القضائية لمُرتكبيها.

بموجب قانون مكافحة جرائم المعلوماتية تُعدُّ الجريمة الإلكترونية جريمة خطيرة يُعاقب عليها بالغرامة والسجن وعقوبات أخرى، كما يُخوّل القانون الحكومة باتخاذ تدابير لمنع الوصول إلى مواقع الويب التي تُعدُّ مُتورِّطةً في الجرائم الإلكترونية.

يمكن تقديم إجابات إضافية من قبل الطلبة

6 ابحث في الإنترنت عن الضوابط الأساسية للأمن السيبراني (ECC)، وأذكر الضوابط الرئيسة لبرنامج التوعية بالأمن السيبراني، والتدريب عليه.

الضوابط الأساسية للأمن السيبراني (ECC): يُعدُّ توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني الهدف الرئيس لهذه المتطلبات التي صُمِّمت بناءً على أفضل الممارسات والمعايير لحماية الأصول المعلوماتية للجهات من التهديدات الداخلية والخارجية وتقليل المخاطر السيبرانية، كما تتناول هذه الضوابط جوانب مختلفة من الأمن السيبراني، بما في ذلك إدارة الأصول وهويات الدخول والصلاحيات، وإدارة حوادث وتهديدات الأمن السيبراني، والتوعية والتدريب بالأمن السيبراني. وتُعدُّ هذه الضوابط ملزمة على جميع الجهات الحكومية في المملكة العربية السعودية، بما في ذلك الوزارات والهيئات والمؤسسات وغيرها، والجهات والشركات التابعة لها، وجهات القطاع الخاص التي لديها بُنى تحتية وطنية حسَّاسة (CNIs) أو تعمل على تشغيلها أو استضافتها؛ وذلك لضمان حماية أنظمة المعلومات الخاصة بها.

ضوابط الأمن السيبراني للبيانات (DCC):أصدرت الهيئة الوطنية للأمن السيبراني (NCA) ضوابط الأمن السيبراني للبيانات لتحسين تنظيم الفضاء السيبراني وأمنه في المملكة، وتَهدف تلك الضوابط إلى رفع مستوى الأمن السيبراني لحماية البيانات الوطنية، وتعزيز الأمن السيبراني للجهات خلال مراحل دورة حياة البيانات وذلك لضمان حماية بياناتها والأصول المعلوماتية من التهديدات والمخاطر السيبرانية.

1. حوكمة الأمن السيبراني	1-1	المراجعة والتدقيق الدوري للأمن السيبراني	1-2	الأمن السيبراني المتعلق بالموارد البشرية
	1-3	برنامج التوعية والتدريب بالأمن السيبراني		
2. تعزيز الأمن السيبراني	2-1	إدارة هويات الدخول والصلاحيات	2-2	حماية الأنظمة وأجهزة معالجة المعلومات
	2-3	أمن الأجهزة المحمولة	2-4	حماية البيانات والمعلومات
	2-5	التشفير	2-6	الإتلاف الآمن للبيانات
	2-7	الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير		
3. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية	3-1	الأمن السيبراني المتعلق بالأطراف الخارجية		

يمكن تقديم إجابات إضافية من قبل الطلبة

7 قَيِّم الآثار المترتبة على النظام الأوروبي العام لحماية البيانات (GDPR) على الشركات العاملة عبر الحدود.

اللائحة العامة لحماية البيانات هي لائحة قانونية تَختصُّ بحماية البيانات والخصوصية في الاتحاد الأوروبي والمنطقة الاقتصادية الأوروبية، وينطبق قانون النظام الأوروبي العام لحماية البيانات (GDPR) على معالجة البيانات الشخصية كليًا أو جزئيًا بالوسائل المؤتمتة، ومعالجتها بغيرها من تلك الوسائل التي تشكل أو ستشكل جزءًا من نظام الملفات.

التشفير في الأمن السيبراني

وصف الدرس

الهدف العام من الدرس هو التعرّف على مقدمة في **علم التشفير** (Cryptography)، وتنفيذ خوارزميات التشفير المختلفة.

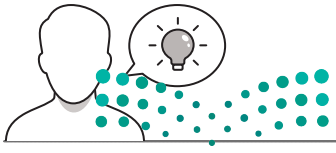
أهداف التعلُّم

- معرفة مبادئ في علم التشفير.
- تنفيذ خوارزميات التشفير المختلفة.

الدرس الثاني	
الوحدة الثالثة: مواضيع متقدِّمة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الثاني: التشفير في الأمن السيبراني	3

نقاط مهمَّة

- قد لا يميّز بعضُ الطلبة بين خوارزمية **تشفير قيصر** (Caesar Cipher)، وخوارزمية **تشفير فيجنر** (Vigenère Cipher)، وضّح لهم الفرق بينهما، ومثّل لكل نوع.
- قد يخفى على بعض الطلبة نظام **آسكي** (ASCII)، وضّح لهم أنه نظام ترميز يتكون من مجموعة رموز قياسية تمثّلُ جميع الأحرف الأبجدية الرقمية الإنجليزية.

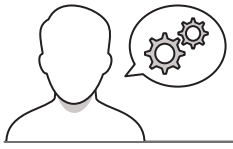


التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- ما ممارسات التشفير في الحضارات السابقة؟
- ما تقنية سلسلة الكُتل (Blockchain)؟ وما تطبيقاتها الشائعة؟
- ما علاقة التشفير بالأمن السيبراني؟



خطوات تنفيذ الدرس

> في البداية ناقش الطلبة حول مفهوم علم التشفير، وتاريخه في الحضارات السابقة.

> اشرح لهم المفهومين الأساسيين لعلم التشفير وهما التشفير، وفك التشفير، والعملية التي تتم في كل منهما.

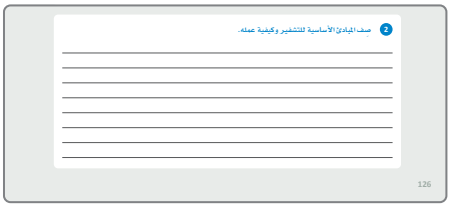
> وضّح أهمية علم التشفير من خلال سرية البيانات، والمصادقة، والسلامة، وعدم الإنكار.

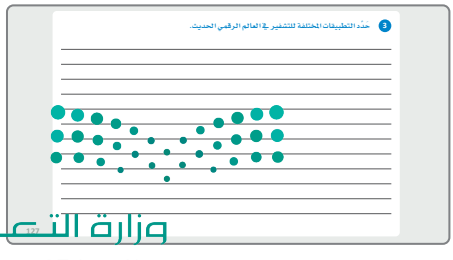
> وجّههم لحل التمرين الثاني؛ للتحقق من فهمهم للمبادئ الأساسية للتشفير، وكيفية عمله.

> استعرض للطلبة تطبيقات التشفير الشائعة، حيث يمكنك الاستعانة بالجدول (3.1) لتوضيح تلك التطبيقات ووصف كل منها.

> اطلب منهم حل التمرين الثالث؛ للتحقق من فهمهم لتطبيقات التشفير الحديثة.


الدرس الثاني
التشفير في الأمن السيبراني
مقدمة في علم التشفير Introduction to Cryptography
أهمية علم التشفير The Importance of Cryptography
علم التشفير هو العلم الذي يختصُّ بالكتابة السرّية بهدف إخفاء المعنى الحقيقي للرسالة. ويهدفُ هذا العلم إلى الحفاظ على المعلومات آمنةً وسريةً باستخدام الترميز والخوارزميات والشفرات. لعلم التشفير تاريخ طويل، حيث تطوّرت أشكاله على مدى التاريخ بدءًا بالشفرات البسيطة المبنيّة على استبدال الحروف التي استخدمتها الحضارات القديمة، إلى خوارزميات التشفير المتطورة المُستخدمة في الاتصالات الرقمية الحديثة. ويعكس تطوره عبر التاريخ الابتكار المستمر والجهود المبذولة لتطوير تقنيات التشفير للاستجابة للاحتياجات المُتغيّرة والتقدُّم التقني.
يعتمدُ علم التشفير في جوهره على مفهومين أساسيين هما: التشفير (Encryption) وفكّ التشفير (Decryption)، حيث يُحوِّل التشفير النص غير المُشفّر والمعلومات القابلة للقراءة إلى نص مُشفّر ومعلومات غير قابلة للقراءة وذلك باستخدام مفتاح سرّي وخوارزمية محدّدة، بينما يعمل فكّ التشفير عكس ذلك. فهو ببساطة عملية تحويل النص المُشفّر مرة أخرى إلى نص غير مشفّر. يُعدُّ علم التشفير أمرًا حيويًا لتأمين الاتصالات وحماية البيانات في عالم يعتمد على الاتصالات بشكل متزايد. وتوضّح النقاط التالية أهمية هذا العلم:
سرّية البيانات (Data Confidentiality):
يقوم التشفير بحماية البيانات الحسّاسة والمعلومات الشخصية والمالية والسرية بحيث لا يتمكّن من الوصول إليها إلا أولئك المُصرّح لهم بذلك باستخدام المفاتيح الصحيحة لفك التشفير. ويُعدُّ هذا ضروريًا للقطاعات الحيوية في الدولة مثل: القطاعات المالية، ومؤسسات الرعاية الصحية، والهيئات الحكومية.
المصادقة (Authentication):
يُتيح التشفير استخدام التوقيعات الرقمية للتحقُّق من صحّة الرسائل، وإنشاء هوية المُرسل، ومنع العبث بالمحتوى أثناء الإرسال.
السلامة (Integrity):
يُساعد التشفير على ضمان سلامة البيانات باستخدام تقنيات متقدّمة للتحقق والكشف أي تغيير.
عدم الإنكار (Non-repudiation):
يُوفّر تقنيات التشفير خاصية عدم الإنكار، مما يضمن عدم تمكّن الأطراف التي تملك إمكانية الوصول إلى البيانات من إنكار مُعاملاتهم أو تداولهم للبيانات. ويُعدُّ هذا الأمر مهمًا في الأغراض القانونية والمالية وغيرها، حيث يكون الحفاظ على سلامة البيانات والمُعاملات أمرًا ضروريًا.
نص غير مشفر
تشفير
مفتاح سري
نص مُشفّر
قناة غير مأمونة
فك التشفير
مفتاح سري
نص غير مشفر
شكل 3.3: تمثيل عملية تشفير وفك تشفير فيزيائية
112


2 صف المبادئ الأساسية للتشفير وكيفية عمله.
126


3 حدّد التطبيقات المختلفة للتشفير في العالم الرقمي الحديث.

> انتقل إلى شرح أنواع التشفير وهي: تشفير المفتاح المتماثل و تشفير المفتاح غير المتماثل، ودوال الاختزال، ثم وضّح الفرق بينها، وأهم الخوارزميات المستخدَمة في كل منها.

> يمكنك توجيه الطلبة لحل التمرينات الرابع والخامس والسادس؛ للتحقق من فهمهم لأنواع التشفير.

التطبيق	الوصف
سلسلة الكتل والعملات الرقمية	يُعدُّ التشفير عُنصرًا أساسيًا في تقنية سلسلة الكتل (Blockchain) والعملات الرقمية (Digital Currencies)، حيث يُستخدم لحماية المعاملات والحفاظ على السجل الموزع (Distributed Ledger)، وضمان موثوقية المشتركين.

أنواع التشفير Types of Cryptography

يُشمل التشفير مجموعة متنوعة من التقنيات يُمكن تصنيفها على نطاق واسع إلى ثلاثة أنواع رئيسة هي: تشفير المفتاح المتماثل (Symmetric Key Cryptography)، وتشفير المفتاح غير المتماثل (Asymmetric Key Cryptography)، ودوال الاختزال (Hash Functions)، بحيث يخدم كل نوع غرضًا مختلفًا، ويتمتع بمزايا وقيود اعتمادًا على متطلبات الأمن ومآلات الاستخدام المحدّدة. وفيما يلي نبذة عن كل نوع من هذه الأنواع:

تشفير المفتاح المتماثل Symmetric Key Cryptography

يستخدم تشفير المفتاح المتماثل أو تشفير المفتاح السري مفتاحًا واحدًا لعمليات التشفير وفك التشفير، وتتمثل وظيفته الرئيسة في التحويل والتبديل. إذا أراد المُرسل إرسال بيانات مُشفّرة، فإنه يستخدم المفتاح السري المشترك لتشفير النص العادي وتحويله إلى نص مُشفّر، ثم يقوم المُستلم الذي يمتلك المفتاح السري نفسه أيضًا بفك تشفير النص المُشفّر مرة أخرى إلى نص غير مُشفّر. يُعدُّ طول المفتاح مهمًا جدًا في تشفير المفتاح المتماثل. ومن أمثلة خوارزميات المفاتيح المتماثلة الشائعة خوارزمية معيار التشفير المتقدم (Advanced Encryption Standard – AES).

شكل 3.4: عملية التشفير باستخدام المفتاح المتماثل

تشفير المفتاح غير المتماثل Asymmetric Key Cryptography

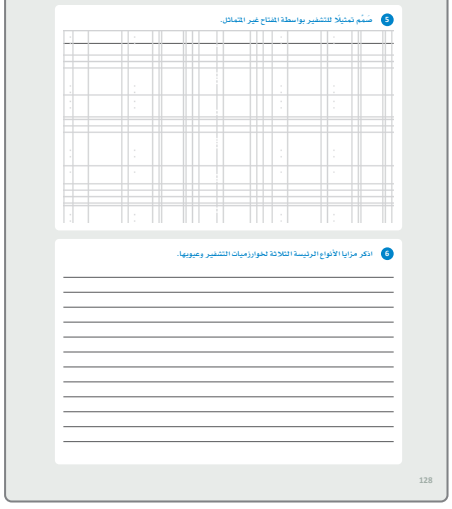
يتضمن تشفير المفتاح غير المتماثل، أو تشفير المفتاح العام، استخدام مفتاحين مختلفين يرتبطان حسابيًا وهما: المفتاح العام (Public Key) والمفتاح الخاص (Private Key)، يتم توزيع المفتاح العام ومشاركته على نطاق عالمية، بينما يبقى المفتاح الخاص سرًا في حوزة المالك، ولا يُمكن الوصول إلى المفتاح الخاص من خلال المفتاح العام. ويجب أن تحظى الجهة التي تُزوّد المُستخدم بالمفتاح العام بالثقة لكي يعمل تشفير المفتاح غير المُتماثل بشكل صحيح. إذا أراد المُرسل تشفير البيانات، فإنه يستخدم المفتاح العام للمُستلم. وعند استلام البيانات المُشفّرة يستخدم المُستلم مفتاحه الخاص لفك تشفير الرسالة. على العكس من ذلك، يُمكن استخدام المفتاح الخاص لتوقيع البيانات لأغراض المصادقة. ويُمكن التحقُّق من التوقيع بواسطة المفتاح العام. تتضمّن بعض خوارزميات المفاتيح غير المتماثلة المُستخدمة على نطاق واسع خوارزمية آر إس إيه (RSA)، وخوارزمية ديفي-هيلمان (Diffie-Hellman)، وخوارزمية التشفير بالمنحنيات الإهليلجية (Elliptic Curve Cryptography – ECC). فمن المهمّ ملاحظة أن طول المفتاح بوحدة البت (Bits) يؤثر بشكل مباشر على أمن التشفير، حيث توفر المفاتيح الأطول حماية أقوى ضد الهجمات.

شكل 3.5: عملية التشفير باستخدام المفتاح غير المتماثل

114

3 حدّد التطبيقات المختلفة للتشفير في العالم الرقمي الحديث.

127



5 صمّم تمثيلًا للتشفير بواسطة المفتاح غير المتماثل.

6 اذكر مزايا الأنواع الرئيسة الثلاثة لخوارزميات التشفير وعيوبها.

128

> انتقل بعدها لشرح طريقتي التحقق من صحة المفاتيح العامة وهما: شبكات الثقة، وهيئة الشهادات، كما يمكنك تقديم حالة لكل نوع لتوضيح نهج طريقة التحقق الخاصة بكل نوع.

> اطلب منهم حل التمرين السابع؛ للتحقق من فهمهم لاستخدام شبكات الثقة في التحقق من صحة المفاتيح العامة.

> اشرح لهم هجمات التشفير، وبيّن أبرز الطرائق التي يستخدمها المتسللون للوصول للبيانات المشفّرة.

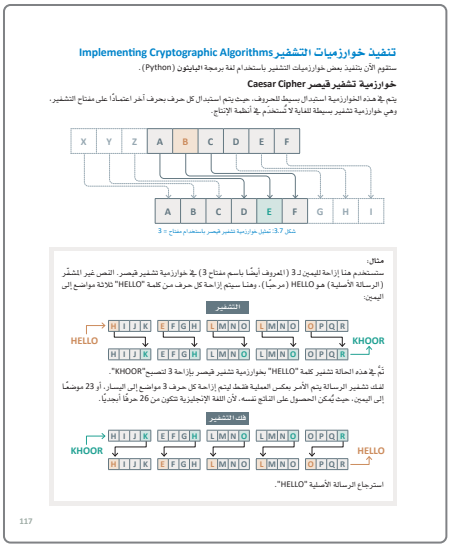
> وجّه الطلبة لحل التمرين الثامن؛ للتحقق من فهمهم لاستخدام المتسللين تحليل الشفرات للوصول إلى البيانات المشفّرة.

7 حلّل كيفية استخدام شبكات الثقة للتحقّق من صحة المفاتيح العامة في التشفير.

8 اشرح كيف يُمكن للمتسللين استخدام تحليل الشفرات للوصول إلى البيانات المُشفّرة.

129

- انتقل بعد ذلك لشرح تنفيذ خوارزميات التشفير، وابدأ بشرح خوارزمية تشفير قيصر، مستعينًا بالمثال الوارد في الكتاب.
- اشرح آلية التشفير بخوارزمية فيجنر، واستعِن بالمثال الوارد في الكتاب لشرحها وتوضيح الفرق بينها وبين خوارزمية تشفير قيصر.
- اشرح لهم خوارزمية ديفي–هيلمان لتبادل المفاتيح، حيث يمكنك الاستعانة بالمثال الوارد في الكتاب؛ لتوضيح آلية فك التشفير من خلالها.
- انتقل إلى شرح علاقة الأمن السيبراني بالتشفير وسلسلة الكتل، ووضّح لهم الطرائق التي يمكن أن تسهم بها السلسلة في تحقيق الأمن السيبراني.
- في الختام وجّه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.



تنفيذ خوارزميات التشفير Implementing Cryptographic Algorithms

سنقوم الآن بتنفيذ بعض خوارزميات التشفير باستخدام لغة برمجة البايثون (Python).

خوارزمية تشفير قيصر Caesar Cipher

يتم في هذه الخوارزمية استبدال بسيط للحروف، حيث يتم استبدال كل حرف بحرف آخر اعتمادًا على مفتاح التشفير. وهي خوارزمية تشفير بسيطة للغاية لا تُستخدم في أنظمة الإنتاج.

شكل 3.7: تمثيل خوارزمية تشفير قيصر باستخدام مفتاح = 3

مثال:

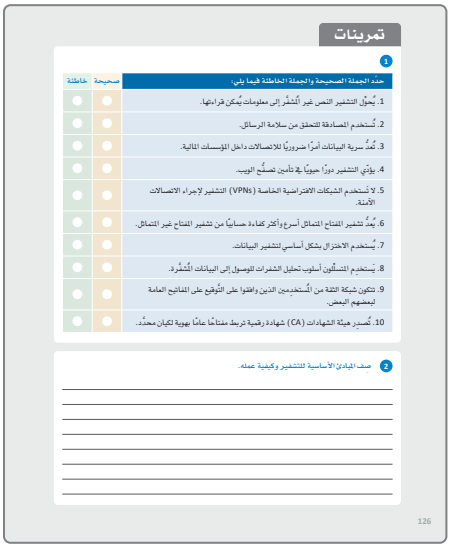
سنستخدم هنا إزاحة لليمين بـ 3 (المعروف أيضًا باسم مفتاح 3) في خوارزمية تشفير قيصر. النص غير المشفّر (الرسالة الأصلية) هو HELLO (مرحبًا). وهنا سيتم إزاحة كل حرف من كلمة "HELLO" ثلاثة مواضع إلى اليمين:

تمّ في هذه الحالة تشفير كلمة "HELLO" بخوارزمية تشفير قيصر بإزاحة 3 لتصبح "KHOOR".

لفك تشفير الرسالة يتم الأمر بعكس العملية فقط ليتم إزاحة كل حرف 3 مواضع إلى اليسار، أو 23 موضعًا إلى اليمين. حيث يُمكن الحصول على الناتج نفسه. لأن اللغة الإنجليزية تتكون من 26 حرفًا أبجديًا.

استرجاع الرسالة الأصلية "HELLO".

117



تمرينات

1

حدد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُحوِّل التشفير النص غير المُشفَّر إلى معلومات يُمكن قراءتها.		
2. تُستخدم المصادقة للتحقق من سلامة الرسائل.		
3. تُعدُّ سرية البيانات أمرًا ضروريًا للاتصالات داخل المؤسسات المالية.		
4. يؤدي التشفير دورًا حيويًا في تأمين تصفُّح الويب.		
5. لا تُستخدم الشبكات الافتراضية الخاصة (VPNs) التشفير لإجراء الاتصالات الآمنة.		
6. يُعدُّ تشفير المفتاح المتماثل أسرع وأكثر كفاءة حسابيًا من تشفير المفتاح غير المتماثل.		
7. يُستخدم الاختزال بشكل أساسي لتشفير البيانات.		
8. يستخدم المتسللون أسلوب تحليل الشفرات للوصول إلى البيانات المُشفَّرة.		
9. تتكون شبكة الثقة من المُستخدمين الذين وافقوا على التوقيع على المفاتيح العامة لبعضهم البعض.		
10. تُصدر هيئة الشهادات (CA) شهادة رقمية تربط مفتاحًا عامًا بهوية لكيان محدَّد.		

2 صف المبادئ الأساسية للتشفير وكيفية عمله.

126

يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُحوِّل التشفير النص غير المُشفَّر إلى معلومات يُمكن قراءتها. يُحوِّل التشفير النص غير المُشفَّر إلى نص مُشفَّر ومعلومات غيرَ قابلة للقراءة.		✓
2. تُستخدم المصادقة للتحقق من سلامة الرسائل. تستخدم المصادقة للتحقُّق من المستخدمين ومنع العَبَث بمحتوى الرسالة.		✓
3. تُعدُّ سرية البيانات أمرًا ضروريًا للاتصالات داخل المؤسسات المالية.	✓	
4. يؤدّي التشفير دورًا حيويًا في تأمين تصفُّح الويب.	✓	
5. لا تَستخدم الشبكات الافتراضية الخاصة (VPNs) التشفير لإجراء الاتصالات الآمنة. يُعَد التشفير جزءًا مهمًا من اتصالات الشبكة الافتراضية الخاصة (VPN).		✓
6. يُعدُّ تشفير المفتاح المتماثل أسرع وأكثر كفاءة حسابيًا من تشفير المفتاح غير المتماثل.	✓	
7. يُستخدم الاختزال بشكل أساسي لتشفير البيانات.	✓	
8. يَستخدِم المتسلِّلون أسلوب تحليل الشفرات للوصول إلى البيانات المُشفَّرة.	✓	
9. تتكون شبكة الثقة من المُستخدِمين الذين وافقوا على التَّوقيع على المفاتيح العامة لبعضهم البعض.	✓	
10. تُصدِر هيئة الشهادات (CA) شهادة رقمية تربط مفتاحًا عامًا بهوية لكيان محدَّد.	✓	

2 صِف المبادئ الأساسية للتشفير وكيفية عمله.

- سرِّية البيانات: يقوم التشفير بحماية البيانات الحسَّاسة والمعلومات الشخصية والمالية والسرية بحيث لا يتمكَّن من الوصول إليها إلا أولئك المُصرَّح لهم بذلك باستخدام المفاتيح الصحيحة لفك التشفير، ويُعدُّ هذا ضروريًا للقطاعات الحيوية في الدولة مثل: القطاعات المالية، ومؤسسات الرعاية الصحية، والهيئات الحكومية.
- المصادقة: يُتيح التشفير استخدام التَّوقيعات الرقمية للتحقُّق من صحَّة الرسائل، وإنشاء هوية المُرسِل، ومنع العَبَث بالمحتوى أثناء الإرسال.
- السلامة: يُساعد التشفير على ضمان سلامة البيانات باستخدام تقنيات متقدِّمة للتحقق واكتشاف أي تغيير.
- عدم الإنكار: تُوفِّر تقنيات التشفير خاصية عدم الإنكار، مما يضمن عدم تَمكُّن الأطراف التي تملك إمكانية الوصول إلى البيانات من إنكار مُعامَلاتهم أو تداولهم للبيانات، ويُعدُّ هذا الأمر مهمًا في الأغراض القانونية والمالية وغيرها، حيث يكون الحفاظ على سلامة البيانات والمُعامَلات أمرًا ضروريًا.

يمكن تقديم إجابات إضافية من قبل الطلبة

3 حَدِّد التطبيقات المختلفة للتشفير في العالم الرقمي الحديث.

المراسلة الآمنة	يُعدُّ التشفير ضروريًا لتأمين قنوات الاتصال بين المُستخدمين مما يضمن سرِّية المحادثات وسلامتها، فعلى سبيل المثال: تستخدم تطبيقات مثل سيجنال (Signal) وواتس آب (WhatsApp) طريقة تشفير تدعى التشفير التام بين الطرفين (End-to-End Encryption – E2EE) لحماية الرسائل من الوصول غير المُصرَّح به أو من التَنصُّت عليها، وباستخدام تلك الطريقة يُمكن للمُستلمين المستهدَفين فقط فكُّ تشفير الرسائل وقراءتها، مما يُوفِّر مستوى عالٍ من الأمن والخصوصية.
أمن البريد الإلكتروني	تُعدُّ بعض تقنيات التشفير مثل تقنية الخصوصية الجيدة (Pretty Good Privacy – PGP) مفيدةً في تأمين اتصالات البريد الإلكتروني، وتقوم هذه التقنية بتشفير الرسائل والمرفقات، مما يضمن سرِّية المحتوى وسلامته، فهي تسمح للمُستلم المستهدَف فقط بالوصول إلى المعلومات وفك تشفيرها، مما يوفِّر أمنًا قويًا للبريد الإلكتروني كوسيلة اتصالات. وتوفِّر هذه التّقنية التوقيعات الرقميّة التي تسهم في التحقُّق من شخصية المُرسِل، مما يؤدي إلى بناء الثقة في عمليات تبادل البريد الإلكتروني.
تصفُّح الويب الآمن	يُعدُّ التشفير الآمن باستخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) ضروريًا لتأمين عملية تَصفُّح الويب، حيث يتم تشفير الاتصال بين متصفح المُستخدم وخادم الويب، مما يوفِّر سرِّية البيانات الحسَّاسة التي يتم تبادلها أثناء التصفح وسلامتها.
أمن التجارة الإلكترونية	يحمي التشفير البيانات الحسَّاسة في التجارة الإلكترونية، حيث يتم تشفير المعلومات المالية المهمة مثل تفاصيل بطاقات الائتمان، مما يضمن السرِّية وعدم الإنكار، كما يُتيح التشفير التحقُّق من موثوقية موقع الويب باستخدام تقنيات مثل كيربيروس (Kerberos)، والبنيَة التحتيَّة للمفاتيح العامة (Public Key Infrastructure – PKI) لتقديم تجربة تسوق آمنة للعملاء.
الشبكة الافتراضية الخاصة	يُستخدم التشفير إلى جانب بروتوكول الإنترنت الآمن (IPsec) في الشبكات الافتراضية الخاصة (VPNs) لإنشاء اتصالات آمنة ومُشفَّرة بين الأجهزة البعيدة والشبكة الخاصة. بروتوكول الإنترنت الآمن (IPsec) هو مجموعة بروتوكولات تُوفِّر المصادقة والتشفير والتحقق من تكامل الاتصالات بين عناوين بروتوكول الإنترنت (IP)، ومع التشفير يضمن هذا البروتوكول سرية البيانات المنقولة عبر الشبكة الافتراضية الخاصة وسلامتها.
أمن إنترنت الأشياء	يؤدّي التشفير دورًا مهمًا في ضمان الاتصال الآمن وحماية البيانات مع النمو السريع لأجهزة إنترنت الأشياء، حيث تقوم تقنيات التشفير الخفيفة بتشفير البيانات المنقولة بين أجهزة إنترنت الأشياء والخوادم الخلفية (Backend Servers).
سلسلة الكُتل والعملات الرقمية	يُعدُّ التشفير عُنصرًا أساسيًا في تقنية سلسلة الكُتل (Blockchain) والعملات الرقمية (Digital Currencies)، حيث يُستخدم لحماية المُعامَلات والحفاظ على السجل الموزع (Distributed Ledger)، وضمان موثوقية المشتركين.

يمكن تقديم إجابات إضافية من قبل الطلبة

4 اذكر الأنواع الثلاثة الرئيسة لخوارزميات التشفير.

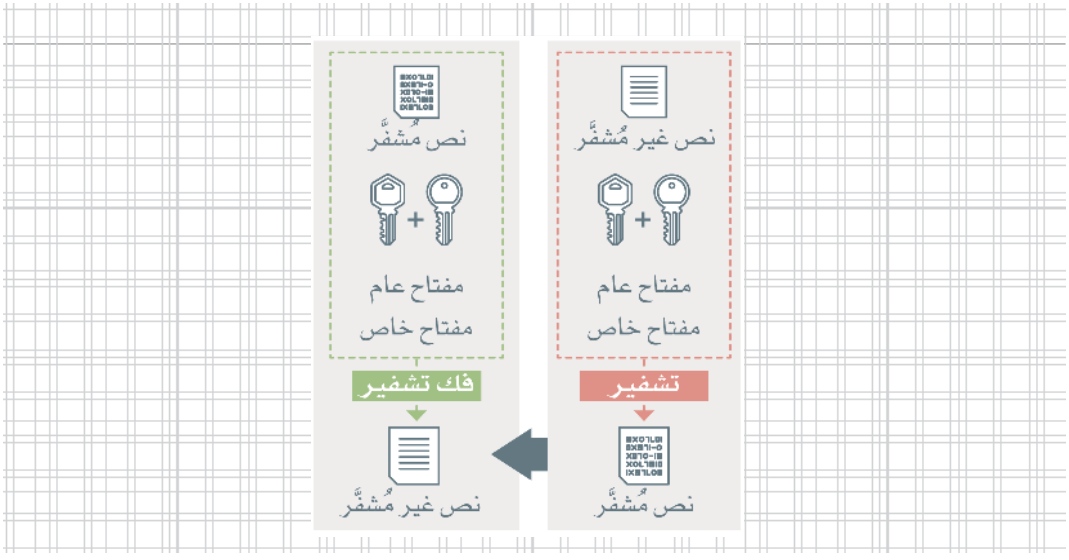
- تشفير المفتاح المتماثل: يَستخدِم تشفير المفتاح المتماثل أو تشفير المفتاح السريّ مفتاحًا واحدًا لعمليات التشفير وفك التشفير، وتتمثل وظيفته الرئيسة في التحويل والتبديل.

- تشفير المفتاح غير المتماثل: يتضمَّن تشفير المفتاح غير المتماثل، أو تشفير المفتاح العام، استخدام مفتاحين مُختلفين يرتبطان حسابيًا وهُما: المفتاح العام (Public Key) والمفتاح الخاص (Private Key).

- دوال الاختزال: هي تقنية تشفيرٍ تقوم بتحويل مُدخَلاتٍ ذات طول عشوائي إلى مُخرَجاتٍ بطولٍ ثابت.

يمكن تقديم إجابات إضافية من قبل الطلبة

5 صَمِّم تمثيلًا للتشفير بواسطة المفتاح غير المتماثل.



6 اذكر مزايا الأنواع الرئيسة الثلاثة لخوارزميات التشفير وعيوبها.

النوع	المزايا	العيوب
تشفير المفتاح المتماثل	أسرع وأكثر كفاءة من الناحية الحسابية. مناسب لتشفير البيانات واسعة النطاق.	تحدِّيات في توزيع المفاتيح وإدارتها. لا يستخدم توقيع رقمي، ولا يضمن صحَّة هويَة المُستخدِم.
تشفير المفتاح غير المتماثل	التوزيع المبسط للمفاتيح (مشاركة المفتاح العام). تمكين التَّوقيعات الرقمية والمصادَقة.	أبطأ وأكثر صعوبة من الناحية الحسابية. أقل ملاءمة لتشفير البيانات واسعة النطاق.
الاختزال	يتميز بالسرعة. من الصعب عمل الهندسة العكسية للعملية. المُخرَجات بطول ثابت بغَضِّ النظر عن طول المُدخَلات.	عُرضَة للتصادم في الخوارزميات الضعيفة، حيث يُمكن لمُدخَلين مختلفين إنتاج المخرَج نفسه.

يمكن تقديم إجابات إضافية من قبل الطلبة

7 حَلِّل كيفية استخدام شبكات الثقة للتحقُّق من صحَّة المفاتيح العامة في التشفير.

شبكات الثِّقة: شبكات الثِّقة هي نهج لامركزي يُستخدَم في التشفير للتحقُّق من صحَّة المفاتيح العامة، ويُمكن تفسير هذا النهج بالمثال التالي:

لنفترض أنّ خالدًا أراد التحقّق من أمان المفتاح العام لأحمد بطريقة لا تعتمد على هيئة شهادات مركزية، وهي فحص شبكة الثقة، ومن خلال ذلك وجد أن فهد - وهو كيان موثوق به على الويب - قد وَقَّع على المفتاح العام لأحمد ليؤكِّد على صحَّته، وبما أن خالدًا يَعرِف فهد ويثقُ به، فيُمكنه الآن الوثوق في أصالة المفتاح العام الذي يخصُّ أحمد، كما لاحظ خالد أن مُستخدِمين آخرين على الويب قد أكَّدوا على مفتاح أحمد، مما زاد من درجة موثوقية الشبكة، وهذا يعني أنه كلما ازداد عدد المُستخدِمين الذين يؤكِّدون صحَّة مفتاح عام، فإنه يصبح أكثر جدارةً بالثقة داخل الشبكة. يساعد هذا النهج اللامركزي في منع الجهات الضارة من استخدام مفاتيح عامة مزيفة أو غير مُصرَّح بها للوصول إلى البيانات المُشفَّرة، ومن خلال الاعتماد على شبكة من الكيانات الموثوقة يعمل التشفير على تعزيز شبكات الثقة للتحقُّق من صحَّة المفاتيح العامة وضمان أمن وسلامة الاتصالات.

8 اشرح كيف يُمكن للمتسلِّلين استخدام تحليل الشفرات للوصول إلى البيانات المُشفَّرة.

يُستخدَم تحليل الشفرات لمعالجة تشفير البيانات للوصول إلى نقاط الضعف في مُخطَّط التشفير التي يُمكن استغلالها لاستخراج البيانات أو تغييرها، حيث يَستخدِم المتسلِّلون هذا التحليل للوصول إلى البيانات المُشفَّرة مثل: كلمات المرور، وأرقام بطاقات الائتمان والمستندات السرية، وغالبًا ما يستخدمون تقنيات لكسر مُخطَّطات التشفير، بما في ذلك الهجمات التحليلية، والقوة المُفرطة، وهجمات القناة الجانبية.

الأمن السيبراني والتقنيات الناشئة

وصف الدرس

الهدف العام من الدرس هو التعرف على أنظمة الأمن السيبراني في التقنيات الناشئة بما في ذلك إنترنت الأشياء، والمُدُن الذكية، والمركبات ذاتية القيادة، وشبكات الجيل الخامس ، والحوسبة السحابية، والحوسبة الكَميَّة، وأنظمة الذكاء الاصطناعي وتعلُّم الآلة، والروبوتات والأنظمة المستقلة ذاتيًا، وتقنيات الواقع المعزز والافتراضي والميتافيرس، بالإضافة للتوائم الرقمية.

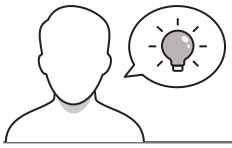
أهداف التعلُّم

- معرفة أنظمة الأمن السيبراني في التقنيات الناشئة وتطبيقاتها.

الدرس الثالث	
الوحدة الثالثة: مواضيع متقدمة في الأمن السيبراني	عدد الحصص الدراسية
الدرس الثالث: الأمن السيبراني والتقنيات الناشئة	3

نقاط مهمَّة

- قد يظن بعض الطلبة أن المركبات ذاتية القيادة لا تكون عُرضة للهجمات السيبرانية، بيّن لهم أن مُرتكبي الجرائم السيبرانية قد يستغلون الثغرات الأمنيّة في نظام اتصالات المركبة؛ مما يسبب تدميرها أو تعريض ركابها للخطر.
- قد لا يدرك بعض الطلبة أهم التطورات التي أحدثتها شبكة الجيل الخامس في مجالات الصناعة والصحة والتعليم وغيرها، وضّح لهم أبرز تلك التطورات، وبيّن أن فائدتها تتعدى استخدامها في الأجهزة المحمولة والألعاب وغيرها.

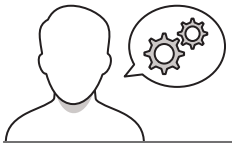


التمهيد

عزيزي المعلّم، إليك بعض الاقتراحات التي يمكن أن تساعدك في تحضير الدرس، والإعداد له، إضافة إلى بعض النصائح الخاصة بتنفيذ المهارات المطلوبة في الدرس:

> اجذب اهتمام الطلبة من خلال طرح الأسئلة التالية:

- هل سبق لكم مشاهدة سيارات ذاتية القيادة؟ وكيف تعمل؟
- ما شبكة الجيل الخامس؟ وما أبرز التطورات التي أحدثتها؟
- ماذا نقصد بتعلُّم الآلة؟ وما أبرز تطبيقاتها في حياتنا؟



خطوات تنفيذ الدرس

> في البداية ناقِش الطلبة حول مفهوم التقنيات الناشئة، وبيّن لهم دور الأمن السيبراني في حماية البيانات والأنظمة والشبكات التي تستعين بها هذه الأنظمة.

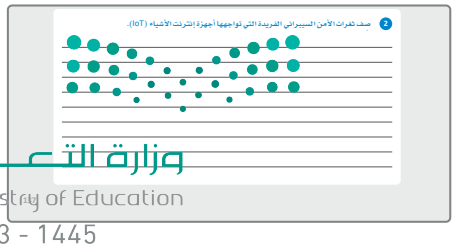
> اشرح لهم مفهوم أجهزة إنترنت الأشياء، وقدّم لهم الأمثلة عليها، ثم بيّن لهم أهم المخاطر التي يمكن أن تتعرض لها، وكيفية الوقاية منها.

> يمكنك توجيه الطلبة لحل التمرين الثاني؛ للتحقق من فهمهم للمخاطر التي يمكن أن تواجه تقنيات إنترنت الأشياء.

> انتقل إلى شرح مفهوم المُدُن الذكية، وقدّم الأمثلة على أبرز تطبيقاتها، ثم وضّح المخاطر التي تهددها، وكيفية الوقاية منها.

> اشرح بعد ذلك المركبات ذاتية القيادة، ووضّح لهم أبرز المخاطر التي يمكن أن تتعرض لها، واطلب منهم اقتراح أهم الممارسات المقترح تنفيذها للوقاية من تلك المخاطر.


الدرس الثالث
الأمن السيبراني والتقنيات الناشئة
www.ien.edu.sa
أنظمة الأمن السيبراني في التقنيات الناشئة
Cybersecurity Systems in Emerging Technologies
تُسهم التقنيات الناشئة في التحوُّل والتطوُّر الكبير والسريع لكثير من مناحي الحياة حول العالم. كما تُشكِّل هذه التقنيات أيضًا تحديات ومخاطر كبيرة على أمن وخصوصية الأفراد والمؤسسات والدول.
تُعدُّ أنظمة الأمن السيبراني ضرورية لحماية البيانات والأنظمة والشبكات التي تستهدفها الهجمات الضارة والحدّ من إمكانيات الوصول غير المُصرَّح به. وفيما يلي نُقدِّمة لبعض الثغرات الأمنيّة المعروفة في التقنيات الناشئة المُستخدمة على نطاقٍ واسع، وسبب أهمية أنظمة الأمن السيبراني في حمايتها:
أجهزة إنترنت الأشياء IoT Devices
إنترنت الأشياء (Internet of Things - IoT) هو شبكة من الأجهزة المترابطة والمستشعرات تجمع البيانات وتنقلها وتتبادلها مع بعضها، وتشمل هذه الأجهزة أنواعاً مختلفة تمتد من الأجهزة المنزلية الذكية مثل: مُنظِّمات الحرارة وأنظمة الحماية، إلى الآلات الصناعية، وأجهزة المراقبة الصحية، والأجهزة القابلة للارتداء، تزداد مساهمة الهجمات المحتملة لمُركبي الجرائم السيبرانية مع تزايد عدد أجهزة إنترنت الأشياء، فعلى سبيل المثال، تمتلك الكثير من هذه الأجهزة في بيئات الحوسبة المتطورة موارد محدودة، مما يحدُّ من قدرتها على تنفيذ إجراءات أمن قوية. ويجعلها أكثر عُرضة للهجمات. يجب أن تتبنى المؤسسات التي تستخدم الحوسبة المتطورة ممارسات أمن سيبراني قوية مثل: التشفير، والإدارة الآمنة للأجهزة، وتجزئة الشبكة لحماية بياناتها وأنظمتها من التهديدات المحتملة. وتتضمّن بعض المخاطر المرتبطة بإنترنت الأشياء، ما يأتي:
ضعف المصادقة والتفويض (Weak Authentication and Authorization):
غالبًا ما تفتقر أجهزة إنترنت الأشياء إلى آليات مصادقة وتفويض قوية، مما يجعلها أهدافًا سهلة للمهاجمين. ولذلك يجب استخدام كلمات مرور قوية والمصادقة متعددة العوامل (MFA) لحماية أجهزة إنترنت الأشياء من الوصول غير المُصرَّح به.
ضعف التشفير (Lack of Encryption):
تفتقر العديد من أجهزة إنترنت الأشياء إلى إمكانيات التشفير القوية، مما قد يُتيح اعتراض البيانات من قِبَل المهاجمين، ولذلك يجب تنفيذ إجراءات تشفير متقدِّمة.
ثغرات البرامج الثابتة (Firmware Vulnerabilities):
البرامج الثابتة (Firmware) هي شكل من أشكال البرامج المُصمَّمة أو المُضمَّنة في الأجهزة لتعمل بفعالية، وغالبًا ما تحتوي أجهزة إنترنت الأشياء على برامج ثابتة يُمكن اختراقها بسهولة، مما يسمح للمهاجمين بالتحكّم في الجهاز.
130


2 صف ثغرات الأمن السيبراني الفريدة التي تواجهها أجهزة إنترنت الأشياء (IoT).

- اشرح لهم تطور شبكات الاتصالات وصولًا للجيل الخامس، وقدّم الأمثلة على أبرز التطورات التي أحدثتها، والمخاطر التي يمكن أن تتعرض لها.
- اطلب من الطلبة حل التمرين الثالث؛ للتحقق من فهمهم للتدابير الأمنيّة التي تساعد على حماية تقنية الجيل الخامس من مخاطر الأمن السيبراني.

- انتقل بعدها لشرح الحوسبة السحابية، ووضّح المخاطر التي تواجهها، وأهم الإرشادات التي تساعد في حمايتها.
- يمكنك بعدها توجيه الطلبة لحل التمرين الخامس؛ للتأكد من فهمهم لنموذج المسؤولية المشتركة الموجود بين مزود الخدمة السحابية وعملائه.
- اشرح لهم مفهوم الحوسبة الكَميَّة، ووضّح أهميتها في المجالات المختلفة، ثم بيّن المخاطر التي تواجهها فيما يتعلق بالأمن السيبراني، ودور الخوارزميات في مقاومة المخاطر المتعلقة بالتشفير.
- وجّه الطلبة لحل التمرين السادس؛ بهدف التحقق من فهمهم لخوارزميات مقاومة الحوسبة السحابية لمخاطر الأمن السيبراني.


إجراء اختبارات صارمة والتحقق من صحّة جميع المكوّنات لتحديد ثغرات الأمن السيبراني وإصلاحها.

تنفيذ مصادقة قوية والتحكم بالوصول لمنع الوصول غير المُصرَّح به إلى الأنظمة المركزية.

وضع خطط شاملة للاستجابة للحوادث والتخفيف منها بسرعة.

التأكد من تطبيق السياسات السليمة للحفاظ على خصوصية البيانات، وأن البيانات يتم جمعها وتخزينها واستخدامها وفقًا للضوابط المحدّدة لذلك.

شبكات الجيل الخامس 5G Networks

تتميز شبكات الجيل الخامس بتوفير خدمات الاتصالات والإنترنت بسُرعات عالية، وزمن وصول أقل، وسعة أكبر لتحميل وتبادل البيانات، مما يتيح ظهور تقنيات حديثة مثل: المركبات ذاتية القيادة، والمُدن الذكية، وتطبيقات إنترنت الأشياء. ومع ذلك، فإن نشر شبكات الجيل الخامس يمثّل تحديات جديدة للأمن السيبراني، حيث أصبحت هناك حاجة ماسة إلى اتخاذ تدابير قوية للأمن السيبراني لحماية البنية التحتيّة أمام زيادة نطاق الهجمات، والمخاطر المُحدقة بسلاسل التوريد، والاستغلال المحتمل لمُكوّنات الشبكة.

أضف إلى ذلك أن تعقيد شبكات الجيل الخامس والعدد الهائل من الأجهزة المتراصة يتيح الفرصة لمُرتكبي الجرائم السيبرانية؛ لاستغلال نقاط الضعف، مما قد يؤدي إلى تعطيل الخدمات المهمة أو سرقة البيانات الحساسة.

الحوسبة السحابية Cloud Computing

تُمكّن الحوسبة السحابية الشركات والأفراد من تخزين بياناتهم ومعالجتها وإدارتها على الخوادم البعيدة، مما يوفر قابلية التوسع وتوفير التكاليف والمرونة، ولكن يتطلب الاعتماد على الخدمات والبنية التحتيّة السحابية تطبيق إجراءات سيبرانية قوية لحماية البيانات والتطبيقات المستضافة سحابيًا، تشمل مخاطر الأمن السيبراني السحابية خروقات البيانات، والوصول غير المُصرَّح به، وسرقة الحسابات، فعلى سبيل المثال: يُمكن لخدمات التخزين السحابية التي تمت تهيئتها بشكل غير صحيح عرض معلومات حساسة للجمهور، مما يؤدي إلى تسرّب البيانات وما يتبع ذلك من العواقب القانونية المحتملة. كما يُمكن أن تُشكّل التهديدات الداخلية خطرًا كبيرًا على البيانات السحابية، حيث يُمكن للمستخدمين ذوي الصلاحيات الواسعة إلى الأنظمة السحابية إساءة استخدام صلاحيات الوصول لسرقة البيانات أو تعطيل الخدمات، تُعدُّ المسؤولية المشتركة لإدارة الحوسبة السحابية مميزًا للقلق، حيث يكون مزود الخدمة السحابية مسؤولًا عن تأمين البنية التحتيّة الأساسية، بينما يكون العميل مسؤولًا عن حماية بياناته وتطبيقاته المُستضافة سحابيًا، ويؤدي تقسيم المسؤولية هذا أحيانًا إلى حدوث ارتباك أو ثغرات أمنية، مما يزيد من احتمالية نجاح الهجمات، ولذلك يجب على المؤسسات فهم مسؤولياتها وتنفيذ إجراءات الأمن المناسبة لحماية أصولها السحابية.

الحوسبة الكَميّة Quantum Computing

تستفيد الحوسبة الكَميّة من مبادئ ميكانيكا الكم لأداء العمليات الحسابية بشكل أسرع من أجهزة الحاسب التقليدية، وتُعدُّ هذه التقنية المتطورة ذات إمكانات هائلة لمختلف الصناعات، بما في ذلك مجالات التشفير، وتطوير الأدوية، والخدمات المالية، ولكن قد تُشكّل أجهزة الحاسب الكَميَّة مخاطر كبيرة تتعلق بالأمن السيبراني، لا سيما في مجال التشفير، حيث يُمكن للتطوير السريع والكبير لأجهزة الحاسب الكَميَّة أن يُتيح لها إمكانية كسر العديد من خوارزميات التشفير الحالية، مما يجعل البيانات المُشفّرة عُرضة لاختراق وهك التشفير، يقوم الباحثون بتطوير خوارزميات جديدة مقاومة للقدرات الحوسبة الكَميَّة على هك التشفير للاستعداد لمواجهة المخاطر المتعلقة بالتشفير في ظل تطور الحوسبة الكَميَّة، حيث يساعد تطبيق هذه الخوارزميات مسبقًا على ضمان سرية البيانات الحساسة وسلامتها.

133

- استمر في الشرح بتوضيح أنظمة الذكاء الاصطناعي وتعلُّم الآلة، وقدّم لهم أبرز الأمثلة العملية لتطبيقاتها في الأمن السيبراني، وأهم التدابير القوية لحمايتها.
- يمكنك توجيه الطلبة لحل التمرين الرابع؛ للتحقق من فهمهم للمخاطر التي تواجه أنظمة الذكاء الاصطناعي وتعلُّم الآلة.
- اشرح لهم الروبوتات والأنظمة المستقلة ذاتيًا، وبيّن لهم مخاطر الأمن السيبراني التي يمكن أن تواجهها وطرائق الوقاية منها.
- اشرح تقنيات الواقع المعزز والواقع الافتراضي والميتافيرس، وبيّن الفرق بين كل منها وأبرز المخاطر التي يمكن أن تواجهها.
- استمر في الشرح بتوضيح مفهوم **التوائم الرقمية** (Digital Twins)، وبيّن أبرز المخاطر التي تواجهها في الأمن السيبراني، وما يجب اتخاذه من قِبل المؤسسات لحمايتها.
- وجّه الطلبة لحل التمرين السابع؛ للتحقق من فهمهم لأنواع المعلومات المخزّنة في التوأم الرقمي ومخاطر استخدامها.
- في الختام يمكنك توجيه الطلبة لحل التمرين الأول؛ للتحقق من فهمهم لأهداف الدرس.


تمرينات

1

حدد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. الأمن السيبراني مهم لحماية البيانات والأنظمة والشبكات من الهجمات الضارة ومن الوصول غير المصرّح به.		
2. تعتمد المُدُن الذكية على البيانات المُجمّعة من المستشعرات والأجهزة لاتخاذ القرارات الفورية.		
3. قد تتأثر المركبات ذاتية القيادة سلبًا بالهجمات السيبرانية.		
4. يُمكن للحوسبة الكمّية كسر خوارزميات التشفير الحالية.		
5. لا تقدّم الحوسبة السحابية تحديات جديدة للأمن السيبراني.		
6. تُشنّ شبكات الجيل الخامس نطاق هجوم أوسع تُرتكبي الجرائم السيبرانية.		
7. لا تتعرضُ أنظمة الذكاء الاصطناعي وتعلُّم الآلة للهجمات العدائية.		
8. لا تُشكّل الروبوتات والأنظمة المستقلة ذاتيًا أي مخاطر أمن سيبراني.		
9. تُعدُّ العقود الذكية آمنة من أي هجمات مُحتملة.		
10. لا تجمع تطبيقات الواقع المعزز والواقع الافتراضي البيانات الشخصية.		

137


7 اشرح نوع المعلومات المُخزّنة في التوأم الرقمي ومخاطر استخدامها.

139

يمكن تقديم إجابات إضافية من قبل الطلبة

تمرينات

1

حدِّدْ الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. الأمن السيبراني مهم لحماية البيانات والأنظمة والشبكات من الهجمات الضارة ومن الوصول غير المُصرَّح به.	✓	
2. تعتمد المُدُن الذكية على البيانات المُجمَّعة من المستشعرات والأجهزة لإتاحة اتخاذ القرارات الفورية.	✓	
3. قد تتأثر المركبات ذاتية القيادة سلبًا بالهجمات السيبرانية.	✓	
4. يُمكن للحوسبة الكَمِّية كسر خوارزميات التشفير الحالية.	✓	
5. لا تقدِّم الحوسبة السحابية تحديات جديدة للأمن السيبراني. تقدِّم تحديات جديدة للأمن السيبراني.		✓
6. تُنشئ شبكات الجيل الخامس نطاق هجوم أوسع لمُرتكبي الجرائم السيبرانية.	✓	
7. لا تتعرضُ أنظمة الذكاء الاصطناعي وتعلُّم الآلة للهجمات العدائية. إنها عرضة للهجمات العدائية.		✓
8. لا تُشكِّل الروبوتات والأنظمة المستقلة ذاتيًا أي مخاطر أمن سيبراني.	✓	
9. تُعدُّ العقود الذكية آمنةً من أي هجمات مُحتملة. تخلق التقنيات الجديدة دائمًا ثغرات أمنيّة جديدة.		✓
10. لا تَجمع تطبيقات الواقع المعزز والواقع الافتراضي البيانات الشخصية. تجمع كميات هائلة من البيانات الشخصية.		✓

يمكن تقديم إجابات إضافية من قبل الطلبة

2 صِف ثغرات الأمن السيبراني الفريدة التي تواجهها أجهزة إنترنت الأشياء (IoT).

- ضعف المصادقة والتفويض: غالبًا ما تفتقر أجهزة إنترنت الأشياء إلى آليات مصادقة وتفويض قوية، مما يجعلها أهدافًا سهلة للمهاجِمين، ولذلك يجب استخدام كلمات مرور قوية والمصادقة متعددة العوامل (MFA) لحماية أجهزة إنترنت الأشياء من الوصول غير المُصرَّح به.

- ضعف التشفير: تفتقر العديد من أجهزة إنترنت الأشياء إلى إمكانات التشفير القوية، مما قد يُتيح اعتراض البيانات من قِبَل المهاجِمين، ولذلك يجب تنفيذ إجراءات تشفير متقدِّمة.

- ثغرات البرامج الثابتة: البرامج الثابتة (Firmware) هي شكل من أشكال البرامج المُصغَّرة أو المُضمَّنة في الأجهزة لتعمل بفعالية، وغالبًا ما تحتوي أجهزة إنترنت الأشياء على برامج ثابتة يُمكن اختراقها بسهولة، مما يسمح للمهاجِمين بالتحكُّم في الجهاز..

- البرمجيات غير المحدَّثة: لم يكن من الشائع وضع عوامل الأمن بالاعتبار عند تصميم أجهزة إنترنت الأشياء، وما زالت الكثير منها تعمل ببرمجيات تشغيل غير محدَّثة تحتوي على ثغرات أمنية معروفة، ولذلك يضمن التحديث المنتظم للبرامج الثابتة والبرمجيات الخاصة بأجهزة إنترنت الأشياء تصحيح الثغرات الأمنيّة المعروفة.

- مخاوف الخصوصية: غالبًا ما تجمع أجهزة إنترنت الأشياء بيانات شخصية حسّاسة مثل: معلومات الموقع، والبيانات الحيوية التي يُمكن استخدامها لأغراض ضارة إذا وقعت في الأيدي الخطأ، ولذلك يجب أن تحدّ المؤسسات من كمية البيانات الشخصية التي يتم جمعها وتخزينها بواسطة أجهزة إنترنت الأشياء لتقليل المخاوف المتعلقة بالخصوصية.

يمكن تقديم إجابات إضافية من قبل الطلبة

3 قَيِّم التدابير الأمنيّة اللازمة لحماية شبكات الجيل الخامس (5G) من التهديدات السيبرانية.

تتميز شبكات الجيل الخامس بتوفير خدمات الاتصالات والإنترنت بسُرعات عالية، وزمن وصول أقل، وسعة أكبر لتحميل وتبادل البيانات، مما يتيح ظهور تقنيات حديثة مثل: المركبات ذاتية القيادة، والمُدُن الذكية، وتطبيقات إنترنت الأشياء. ومع ذلك، فإن نشر شبكات الجيل الخامس يمثِّل تحديات جديدة للأمن السيبراني، حيث أصبحت هناك حاجة ماسة إلى اتخاذ تدابير قوية للأمن السيبراني لحماية البنيَة التحتيَّة أمام زيادة نطاق الهجمات، والمخاطر المُحدِقة بسلاسل التوريد، والاستغلال المحتمل لمُكوِّنات الشبكة.

4 قَدِّم أمثلة على مخاطر الأمن السيبراني المرتبطة بأنظمة الذكاء الاصطناعي وتعلُّم الآلة.

يُمكن لمُرتكبي الجرائم السيبرانية استهداف هذه الأنظمة ومحاولة التحايل عليها، أو اختراقها لأغراض ضارة، كما يُمكن للمتسلِّلين استخدام تعلُّم الآلة والتقنيات الأخرى القائمة على الذكاء الاصطناعي لتحديد الثغرات الأمنيّة للأنظمة وشن هجمات أكثر تعقيدًا. على سبيل المثال: يُمكن للمهاجِمين استخدام خوارزميات تعلُّم الآلة لإنشاء رسائل بريد إلكتروني احتيالية ذات محتوى احترافي مُقنِع، أو تجاوز ضوابط الأمن بانتحال شخصية مُستخدِمين موثوقين.

إحدى المخاطر المحتملة الأخرى المرتبطة بأنظمة الذكاء الاصطناعي وتعلُّم الآلة هي الهجمات العدائية، حيث يُنشئ مُرتكبي الجرائم السيبرانية مُدخَلات ضارة مُصمَّمة لخداع أو استغلال الثغرات الأمنيّة في نماذج الذكاء الاصطناعي. على سبيل المثال: قد يُضيف المهاجِم تشويشًا خفيفًا إلى صورة، مما قد يتسبب في إخفاق نظام معالجة الصور في التعرف على المُستخدِمين، والمثال الآخر هو التحايل على الخوارزميات الخاصة بمنصَّات التواصل الاجتماعي، حيث يُمكن للمهاجِم نشر معلومات خاطئة، أو إنشاء ملفات شخصية مزيفة، وذلك بهدف التأثير على سلوك المُستخدِمين.

5 قَيِّم نموذج المسؤولية المشتركة الموجود بين مزود الخدمة السحابية وعملائه.

يكون مزود الخدمة السحابية مسؤولًا عن تأمين البنيَة التحتيَّة الأساسية، بينما يكون العميل مسؤولًا عن حماية بياناته وتطبيقاته المُستضافة سحابيًا، ويؤدي تقسيم المسؤولية هذا أحيانًا إلى حدوث ارتباك أو ثغرات أمنية، مما يزيد من احتمالية نجاح الهجمات، ولذلك يجب على المؤسسات فهم مسؤولياتها وتنفيذ إجراءات الأمن المناسبة لحماية أصولها السحابية.

يمكن تقديم إجابات إضافية من قبل الطلبة

6 صِف الحاجة إلى تطوير خوارزميات مقاومة للحوسبة الكَمِّية.

قد تُشكِّل أجهزة الحاسب الكَميَّة مخاطر كبيرة تتعلق بالأمن السيبراني، لا سيما في مجال التشفير، حيث يُمكن للتطوير السريع والكبير لأجهزة الحاسب الكَميَّة أن يُتيح لها إمكانية كسر العديد من خوارزميات التشفير الحالية، مما يجعل البيانات المُشفَّرة عُرضة للاعتراض وفك التشفير.

7 اشرح نوع المعلومات المُخزَّنة في التوأم الرقمي ومخاطر استخدامها.

التوائم الرقمية هي نُسخ افتراضية متماثلة للأصول المادية أو الأنظمة أو العمليات التي يُمكن استخدامها للمحاكاة والتحليل والتحسين، ولهذه النماذج الرقمية تطبيقات مختلفة، بما فيها المُدُن الذكية والتصنيع والرعاية الصحية، ونظرًا لأن التوائم الرقمية أصبحت أكثر ترابطًا، وأكثر قدرةً على تخزين كميات هائلة من البيانات الحسَّاسة، فقد أصبحت أهدافًا رئيسة لمُرتكبي الجرائم السيبرانية. تشمل مخاطر الأمن السيبراني المحتملة للتوأم الرقمي عمليات الوصول غير المُصرَّح به، والتلاعب بالبيانات، والهجمات على البنيَة التحتيَّة الأساسية الداعمة له. على سبيل المثال، يُمكن للمهاجِم التلاعب ببيانات التوأم الرقمي لإحداث اضطرابات تشغيلية أو خِداع مُتَّخِذي القرار، ولحماية التوائم الرقمية من التهديدات السيبرانية يجب على المؤسسات تنفيذ ضوابط وصول قوية، وتشفير البيانات، والمراقبة المستمرة لضمان أمن أصولهم الرقمية وسلامتها.

المشروع

أهداف المشروع:

- عرْض لمحة عامة عن مدينة ذكية ومكوناتها وفوائدها.
- تحديد التحديات الرئيسة للأمن السيبراني للمُدُن الذكية.
- تحليل المكونات المختلفة للمُدُن الذكية، وتحديد تدابير الأمن السيبراني المطلوبة لحمايتها.
- تحديد التقنيات والأدوات والاستراتيجيات الناشئة التي تُعزِّز وضع الأمن السيبراني في المُدُن الذكية.
- تلخيص النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية، وإعدادها في عرض تقديمي.

- قسّم الطلبة لمجموعات متكافئة، واطلب منهم تخطيط المشروع قبل البدء فيه.
- وجّههم للرجوع للمفاهيم النظرية والخطوات العملية في الوحدة عند الحاجة.
- ضع معايير مناسبة لتقييم أعمال الطلبة في المشروع، وتأكّد من فهم لمتطلبات المشروع.
- يمكنك الاسترشاد بمعايير تقييم المشاريع الواردة في الدليل العام.
- قيّمهم وَفْقَ معايير التقييم، وقدّم لهم التغذية الراجعة للوصول لأفضل نتيجة.
- أخيرًا، حدِّد موعد تسليم المشروع ومناقشة أعمال المجموعات.

سُلّم التقدير

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
المعرفة: عرْض لمحة عامة عن مدينة ذكيّة، ومكوناتها، وفوائدها للحكومات، والمواطنين	لم يعرض لمحة عامة عن مدينة ذكيّة، ومكوناتها، وفوائدها للحكومات، والمواطنين.	عرَضَ فقرة واحدة عن مدينة ذكيّة، ومكوناتها، وفوائدها للحكومات، والمواطنين.	عرَضَ فقرتين عن مدينة ذكيّة، ومكوناتها، وفوائدها للحكومات، والمواطنين.	عرَضَ ثلاث فقرات فأكثر عن مدينة ذكيّة، وفوائدها للحكومات، والمواطنين.
المعرفة: تحديد التحديات الرئيسة للأمن السيبراني للمُدُن الذكية، ووصفها	حدَّدَ تحديًا واحدًا أو لم يحدِّد شيئًا من التحديات الرئيسة، ولم يصفها.	حدَّدَ ما بين تحديين إلى ثلاثة تحديات، ولم يصفْها.	حدَّدَ ما بين أربعة إلى خمسة تحديات، ولم يصفْها.	حدَّدَ أربعة تحديات أو أكثر، ووَصَفَها.
المعرفة: تحليل مكونات المختلفة للمُدُن الذكية، وتحديد تدابير الأمن السيبراني المطلوبة لحمايتها	لم يحلِّل أي مكوّن، ولم يذكر التدابير.	حلَّلَ مكوّنًا واحدًا، ولم يذكر التدابير الأمنيّة له.	حلَّلَ مكوّنين، ولم يذكر التدابير الأمنيّة لهما.	حلَّلَ ثلاثة فأكثر من المكونات، وحدَّدَ التدابير الأمنيّة لها.
المعرفة: تحديد التقنيات والأدوات والاستراتيجيات الناشئة التي تُعزِّز وضع الأمن السيبراني في المُدُن الذكية	لم يحدِّد أي تقنية تُعزِّز الأمن السيبراني في المُدُن الذكية.	حدَّدَ واحدة من تقنيات تعزيز الأمن السيبراني في المُدُن الذكية.	حدَّدَ تدبيرين يحتاج فريق الاستجابة للحوادث إلى تنفيذهما مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.	حدَّدَ ثلاثة فأكثر من التدابير التي يحتاج فريق الاستجابة للحوادث إلى تنفيذها مع الأجهزة غير المتصلة بالشبكة للتأكد من عدم إصابتها.
المهارة: تلخيص النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية، وإعدادها في عرض تقديمي	لم يلخِّص النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية، ولم يعدّها في عرضٍ تقديمي.	لخَّصَ واحدة من النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية، ولم يعدّها في عرضٍ تقديمي.	لخَّصَ اثنتين من النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية ولم يعدّها في عرضٍ تقديمي.	لخَّصَ ثلاث فأكثر من النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية، وأعدّها في عرضٍ تقديمي.

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
التفكير الناقد	لا يظهر فهمًا للمشكلة أو أهداف المهمة، وينظر لها بشكل سطحي، ويقبل المعلومات من غير تقييم لمصداقيتها.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد بعض الجوانب لما يجب معرفته وطرح الأسئلة. يحاول دمج المعلومات التي تم جمعها. يدرك أهمية مصداقية المعلومات لكن لا يتخذ إجراءات للتأكد من ذلك.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد بعض الجوانب لما يجب معرفته وطرح الأسئلة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها. يقيم الحجج من خلال تقييم الأدلة الداعمة لها.	يظهر فهمًا للمشكلة أو أهداف المهمة من خلال تحديد ما يجب معرفته، وطرح الأسئلة حسب الحاجة والنظر في وجهات النظر المختلفة. يدمج المعلومات التي تم جمعها ويقيم مصداقيتها، ويميز بين الحقيقة والرأي. يقيم الحجج من خلال تقييم الأدلة الداعمة لها. ويبرر سبب القبول أو الرفض وفق معايير محددة وواضحة.
الإبداع	يولد عددًا محدودًا من الأفكار التي لا ترتبط بالمشكلة أو أهداف المهمة. المنتج نسخة لأمثلة أو إجابات نموذجية سابقة.	يولد عددًا محدودًا من الأفكار التي قد ترتبط بالمشكلة أو أهداف المهمة. المنتج نسخة لأمثلة أو إجابات نموذجية سابقة أو يتضمن توظيف أكثر من طريقة معروفة مسبقًا.	يولد عددًا محدودًا من الأفكار ذات الصلة المباشرة بالمشكلة أو أهداف المهمة. يتضمن المنتج بعض الجوانب المبتكرة، ويتصف بالفائدة العملية.	يولد عددًا من الأفكار ذات الصلة المباشرة بالمشكلة أو أهداف المهمة، ويستخدمها لتطوير حل للمشكلة أو تحقيق أهداف المهمة. يتصف المنتج بالأصالة والابتكار والفائدة العملية.
العمل مع الآخرين	غير مستعد للعمل والتعاون مع الآخرين، لا يشارك في حل المشكلات أو طرح الأسئلة أو المناقشات.	يقوم ببعض المهام في المشروع ويتعاون مع الفريق، ولكن قد لا يساهم بنشاط في حل المشكلات أو طرح الأسئلة أو المناقشات.	يقوم بأداء مهامه في المشروع، يتعاون مع الفريق ويساهم في حل المشكلات وطرح الأسئلة والمناقشات، ويعطي ملاحظات لمساعدة الفريق.	يقوم بأداء مهامه في المشروع ويكملها في الوقت المحدد، يتعاون مع الفريق ويساهم في حل المشكلات وطرح الأسئلة والمناقشات بناءً على الأدلة، ويعطي ملاحظات بناءة لمساعدة الفريق وتحسين العمل.

المستويات / المحكات	ضعيف	جيد	جيد جدًا	متميز
العرض	لا يفي بمتطلبات ما يجب تضمينه في العرض، لا يقدم معلومات واضحة، يستخدم أسلوبًا غير مناسب لأهداف المهمة والجمهور.	يلبي بعض المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة)، يقدم بعض المعلومات الواضحة، ويستخدم أسلوبًا مناسبًا نوعًا ما لأهداف المهمة والجمهور.	يفي بمعظم المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة واضحة)، يقدم المعلومات بوضوح، ويستخدم أسلوبًا مناسبًا لأهداف المهمة والجمهور.	يفي بجميع المتطلبات لما يجب تضمينه في العرض التقديمي (توجد مقدمة وخاتمة واضحة ومثيرة للاهتمام، ينظم الوقت بشكل جيد)، يقدم جميع المعلومات بوضوح ودقة وفق تسلسل منطقي، ويستخدم أسلوبًا مناسبًا لأهداف المهمة والجمهور.

تلميح: محكات المعرفة والمهارات تعتبر أساسية لاستيفاء أهداف المشروع بينما يمكن للمعلّم استخدام محكات (التفكير الناقد / الإبداع / العمل مع الآخرين / العرض) حسب ما يراه مناسب.