وزارة التعليم

## الوحدة الأولى الدرس الأول

# أساسيات الأمن السيبراني

الفصل الدراسي الأول 1447 هـ

من مقرر الأمن السيبراني

وزارة التعليم

# بيانات الدرس

| رقم الدرس | عنوان الدرس | عدد الحصص | صفحات الكتاب<br>الحصة الأول |
|---|---|---|---|
|  |  |  |  |
| الدرس الأول | مقدمة في الأمن السيبراني | حصتان | من صفحة: 9<br>إلى صفحة: 12 |

وزارة التعليم

# الإستراتيجيات

وزارة التعليم

# من خلال العنوان الدرس

## مقدمة في الأمن السيبراني

نقوم بتعبئة الخانتين على اليمين

| ماذا أعرف ؟ | ماذا أريد أن أعرف ؟ | ماذا تعلمت ؟ | كيف أتعلم المزيد ؟ |
| --- | --- | --- | --- |
| | | | |

وزارة التعليم

# تمهيد الدرس

الوحدة الأولى/ الدرس الأول

## مقدمة في الأمن السيبراني

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

# مغامرة علي في عالم الأمن السيبراني

في يوم من الأيام، كان علي يتصفح الإنترنت في منزله، عندما دخل فجأة إلى موقع غريب. فزع عندما ظهرت له نافذة تطلب منه إدخال كلمة المرور الخاصة به. فكر قليلاً وقال: "ماذا لو كانت هذه خدعة؟"

ذهب علي إلى والدته وأخبرها بما حدث. قالت له: "يا بني، هذا يسمى هجوم سيبراني. في عالم الإنترنت، هناك مخاطر مثل هذه التي قد تحاول سرقة معلوماتك."

فاجأ علي وسأل: "لكن كيف أستطيع حماية نفسي؟"

ابتسمت والدته وقالت: "أول خطوة هي أن تستخدم كلمات مرور قوية وفريدة. لا تكرر كلمة مرور واحدة في مواقع كثيرة."

ثم أكملت: "استخدام التحقق الثنائي هو شيء مهم أيضًا. عندما تضيف طبقة أمان إضافية، فإنك تجعل من الصعب على أي شخص الوصول إلى حسابك حتى لو اكتشف كلمة مرورك."

وأضافت: "يجب عليك أيضًا أن تكون حذرًا من الرسائل المريبة أو الروابط التي تبدو مشبوهة. ولا تنسَ تحديث جهازك بشكل دوري."

فكر علي وقال: "إذن يجب أن أكون دائمًا يقظًا وألا أشارك معلوماتي مع أي شخص عبر الإنترنت."

أجابته والدته: "بالضبط، حماية نفسك على الإنترنت جزء من الأمان السيبراني. عليك أن تكون ذكيًا في كل خطوة."

منذ ذلك اليوم، أصبح علي أكثر حرصًا على استخدام الإنترنت بأمان وبدأ يعلم أصدقائه نصائح الأمن السيبراني.

وزارة التعـــليم

# النشاط الإثرائي

وزارة التعليم

# مفردات الدرس

- الأمن السيبراني
- تهديدات الأمن السيبراني
- هجمات السيبرانية
- مثلث أمن المعلومات

وزارة التعليم

# ماذا سنتعلم ؟

- الأمن السيبراني.
- تهديدات الأمن السيبراني.
- الهجمات السيبرانية.
- تاريخ الأمن السيبراني.
- المقصود بمثلث أمن المعلومات.
- التوقيع الرقمي.

## ربط بالوطن

يعتبر الأمن السيبراني جزءًا لا يتجزأ من الأمن القومي لأي دولة، حيث يرتبط بحماية البنية التحتية الحيوية والمعلومات الحساسة للحكومة والقطاعات الحيوية الأخرى. يجب على الدول تبني استراتيجيات شاملة للتصدي للهجمات السيبرانية والتجسس الإلكتروني وضمان سلامة بياناتها.

# الوحدة الأولى - الدرس الأول
## مقدمة في الأمن السيبراني

**ص: ٩** ١- ما المقصود بالأمن السيبراني؟

**ص: ٩** ٢- ما المقصود بتهديدات الأمن السيبراني؟

**ص: ٩** ٣- ما المقصود بالهجمات السيبرانية؟

**ص: ١٠** ٤- ماذا تعرف عن تاريخ الأمن السيبراني؟

**ص: ١١** ٥- ما المقصود بمثلث أمن المعلومات؟ مع الشرح؟



وزارة التعليم

# ورقة العمل

# عرض محتوى الكتاب

## المقصود من الأمن السيبراني

أضحى مجال الأمن السيبراني مهما بشكل متزايد في السنوات الأخيرة ، خاصة مع الاندماج الكبير للتقنية في الحياة اليومية ، فمع ظهور الانترنت وانتشار أجهزة الحاسب والاجهزة المحمولة ، أصبح الأمن السيبراني ضروريا لحماية المعلومات الحساسة وضمان حماية الأنشطة عبر الإنترنت وأمنها ، حيث يشمل مجال الأمن السيبراني مجموعة من الممارسات والتقنيات المصممة للحماية من التهديدات والهجمات السيبرانية

صفحة: 09

# عرض محتوى الكتاب


## المقصود تهديدات الأمن السيبراني

تتمثل هذه التهديدات في أي ظرف أو حدث قد يؤثر سلبا على العمليات ، أو الأصول التنظمية ،أو الأفراد من خلال نظام معلومات عبر الوصول غير المصرح به، أو تخريب والإفصاح عن المعلومات وتغييرها ،أو حجب الخدمة.

صفحة: 09

# عرض محتوى الكتاب

## المقصود بالهجمات السيبرانية

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

# عرض محتوى الكتاب

## تاريخ الأمن السيبراني

يرجع تاريخ الأمن السيبراني إلى السبعينيات من القرن العشرين ،عندما تم تطوير شبكات الحوسبة ،حيث ظهرت فيروسات الحاسب في العام 1986 ،وتسببت بتلف البيانات والأنظمة ،ولذلك تم تطوير جدران الحماية والتشفيرلمكافحة الهجمات السيبرانية ،حيث تتحكم جدران الحماية في حركة البيانات ويحمي التشفير البيانات والمعلومات،وعلى الرغم من التطور المستمر في أنظمة الحماية الجديدة ،إلا أن مرتكبي الجرائم السيبرانيةيجدون طرائق لتجاوزها.

لقد شهد القرن الحادي والعشرون زيادة كبيرة في الهجمات السيبرانية واسعة النطاق والتي عرَّضت الحكومات والشركات والأفراد للخطر، ومن أشهر أمثلة تلك الهجمات: خرق بيانات مؤسسة إكويفاكس (Equifax) عام 2017 الذي كشف البيانات الشخصية لأكثر من 140 مليون شخص، وهجوم سولارويندز (SolarWinds) عام 2020 الذي أثر على العديد من الوكالات الحكومية الأمريكية والشركات الخاصة، ويوضح الشكل 1.2 بعض أكبر خروقات البيانات في التاريخ، ومع تقدُّم التقنية واندماجها المتزايد في الحياة، تتزايد الحاجة إلى الأمن السيبراني.

وفي السنوات الماضية، انتشر التعليم والتوعية بمجال الأمن السيبراني على نطاق واسع، وقد طوَّرت الحكومات والمؤسسات العمل وإرشادات خاصة بهذا المجال لمساعدة الأفراد والشركات على حماية أنفسهم من التهديدات السيبرانية، وتزايد الطلب على متخصصي الأمن السيبراني، وتنوعت فرص العمل المتعلقة بهذا المجال، ومع ازدياد تعقيد الهجمات السيبرانية، تستمر الحاجة إلى المتخصصين المهرة الذين يمكنهم مواجهة هذه الهجمات.

# عرض محتوى الكتاب

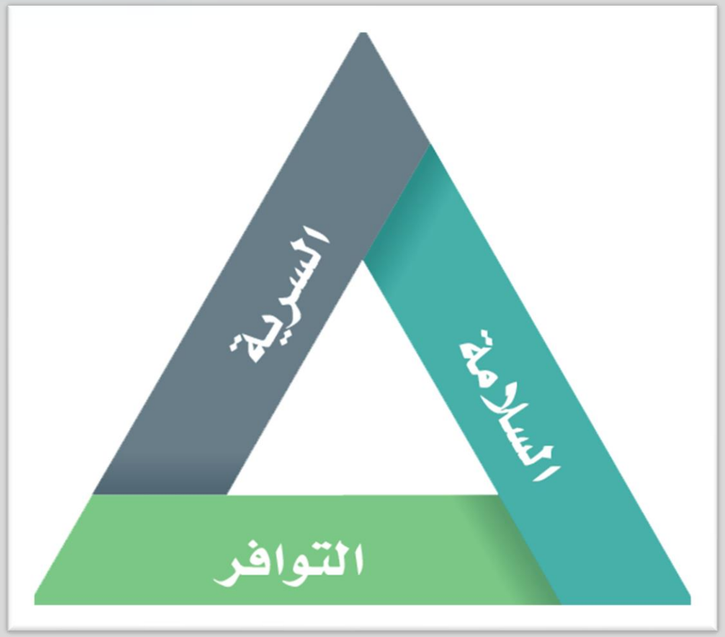
## المقصود بمثلث أمن المعلومات

مثلث الأمن المعلومات ( The CIA Triad) هو نموذج مُستخدَم على نطاق واسع لتصميم سياسات وممارسات الأمن السيبراني وتنفيذها، حيث يشير الاختصار CIA إلى

السرية ( Confidentiality - C)

السلامة (Integrity – I)

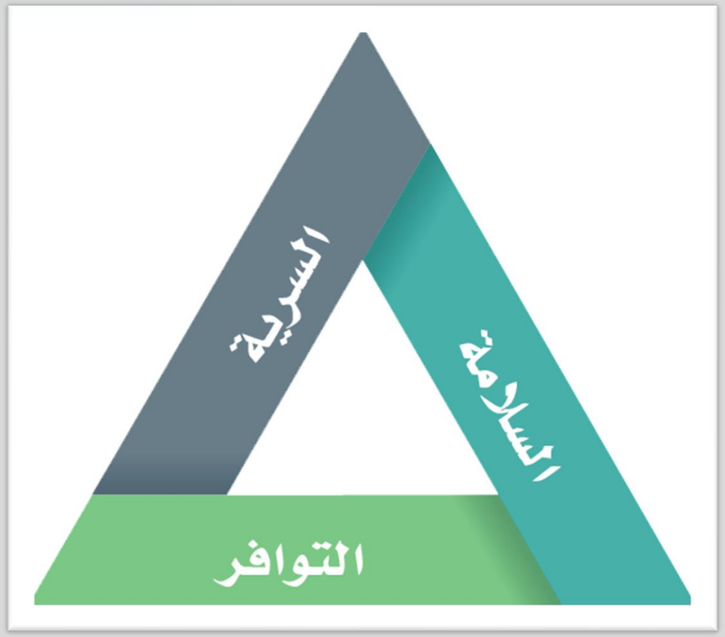
التوافر (Availability – A)




صفحة: 11

# عرض محتوى الكتاب

## المقصود بمثلث أمن المعلومات

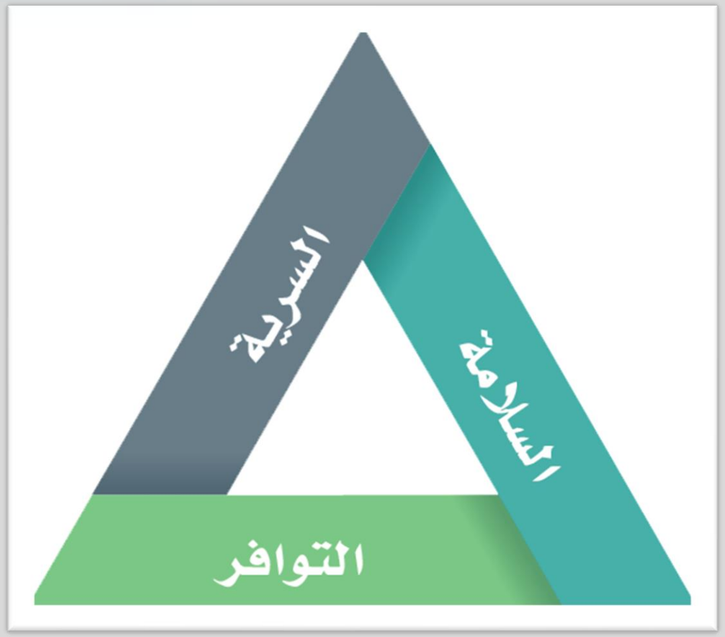



تشير السرية (Confidentiality) إلى الحفاظ على القيود المصرح بها للوصول إلى المعلومات، أي عدم السماح بالوصول للبيانات لمن لا يحق لهم الوصول إليها، ويمكن الحفاظ على السرية من خلال طرائق مختلفة مثل: التشفير، والتحكم في الوصول، وإخفاء البيانات وتواجه السرية تهديدات محتملة مثل: هجمات التصيد الإلكتروني، حيث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

# عرض محتوى الكتاب

## المقصود بمثلث أمن المعلومات

تشير السلامة (Integrity) إلى توكيد دقة البيانات وعدم التلاعب بها ، حيث إن سلامة البيانات ضرورية للحفاظ على الثقة في أنظمة المعلومات، فبدونها لا يمكن للمستخدمين الوثوق بدقة المعلومات التي يتلقونها ، ويُمكن أن تساعد اجراءات مثل: التشفير والتوقيعات الرقمية في ضمان سلامة البيانات، ويُعد اعتراض البيانات بين طرفين من الأمثلة الشائعة على تهديدات سلامة البيانات، حيث يمكن للمهاجم من خلال اعتراض البيانات التسلل إلى شبكة واي فاي (Wi-Fiاللاسلكية غير الآمنة والتلاعب بحزم البيانات التي يتم إرسالها ، وتغيير المحتوى دون علم المرسل أو المستلم.

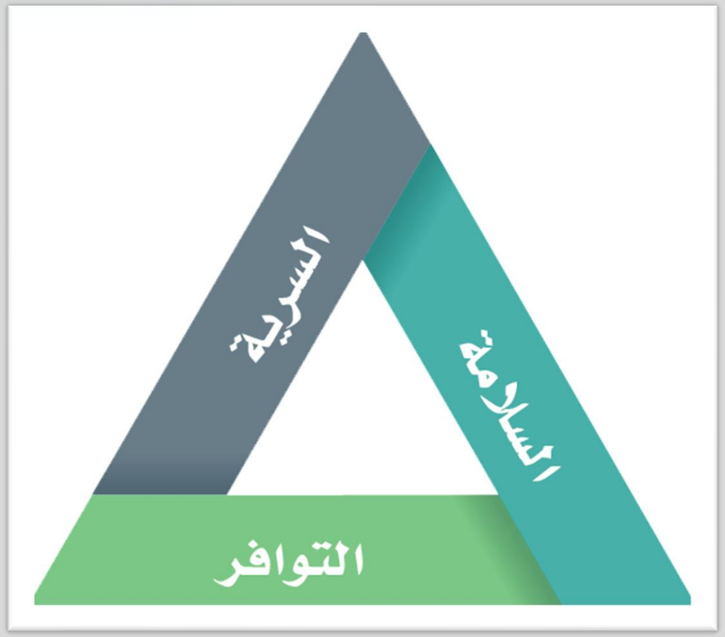



صفحة: 11

# عرض محتوى الكتاب

## المقصود بمثلث أمن المعلومات

يشير التوافر (Availability) إلى ضمان إمكانية الوصول إلى المعلومات عند الحاجة، ويُعد ضروريا لضمان إتاحة الأنظمة والخدمات للمستخدمين عند الحاجة كما يمكن أن يساعد تخزين نسخ متعددة من البيانات، وعمل النسخ الاحتياطية ووضع خطط استعادة القدرة على العمل بعد الكوارث في ضمان التوافر، تعد هجمات حجب الخدمة ( Denial of Service - DoS) طريقة شائعة للمهاجمين لعرقلة توافر البيانات؛ وذلك بإغراق الشبكة بحركة كميات كبيرة من البيانات مما يتسبب في توقف العمليات.




صفحة: 12

# عرض محتوى الكتاب

## التوقيع الرقمي

التوقيع الرقمي هو أحد أنواع التوقيع الإلكتروني يستخدم خوارزميات رياضية للتحقق من صحة رسالة أو مستند أو معاملة وسلامتها.

صفحة: 12

# مهارة التفكير

وزارة التعليم


كيف نميز بين عناصر مثلث أمن المعلومات؟

# النشاط الصفي

**تدريب 5 صفحة: 18**

**تدريب ٥**

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

# ماذا تعلمنا خلال الدرس ؟

- ما المقصود بالأمن السيبراني؟
- ما المقصود بتهديدات الأمن السيبراني؟
- ما المقصود بالهجمات السيبرانية؟
- ماذا تعرف عن تاريخ الأمن السيبراني؟
- ما المقصود بمثلث أمن المعلومات؟ مع الشرح؟
- ما المقصود بالتوقيع الرقمي؟

وزارة التعليم

# الواجب المنزلي

## للمجموعة

تدريب: 3 صفحة: 17

**تدريب ٣**

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


# ختام
# الحصة الأولى

وزارة التعليم

# بيانات الدرس

| رقم الدرس | عنوان الدرس | عدد الحصص | صفحات الكتاب<br>الحصة الثانية |
|---|---|---|---|
|  |  |  |  |
| الدرس الأول | مقدمة في الأمن السيبراني | حصتان | من صفحة: 12<br>إلى صفحة: 15 |

وزارة التعليم

# الواجب المنزلي

## للمجموعة

تدريب: 3 صفحة: 17

**تدريب ٣**

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

مثلث أمن المعلومات: هو نموذج مستخدم على نطاق واسع لتصميم سياسات وممارسات الأمن السيبراني وتنفيذها.

- السرية: تشير إلى الحفاظ على القيود المصرح بها للوصول للمعلومات أي عدم السماح بالوصول للبيانات لمن لا يحق لهم الوصول إليها.
- السلامة: تشير إلى توكيد دقة البيانات وعدم التلاعب بها.
- التوافر : تشير إلى ضمان إمكانية الوصول إلى المعلومات عند الحاجة.

وزارة التعليم

# النشاط الإثرائي

وزارة التعليم

# مفردات الدرس

- الأدوار الوظيفية
- الحوكمة
- الكوادر
- تقييم الثغرات

# ماذا سنتعلم ؟

- الأدوار الوظيفية في الأمن السيبراني.
- دور الحكومة السعودية في الأمن السيبراني.
- المبادرات المهنية للأمن السيبراني في السعودية.

مادة المهارات الرقمية

ص: ١٣ ٦- ما المقصود بالتوقيع الرقمي؟

ص: ١٣ ٧- ما الأدوار الوظيفية في الأمن السيبراني؟

ص: ١٤ ٨- ما الدور المقدم من الحكومة السعودية نحو الأمن السيبراني؟

ص: ١٥ ٩- ما أبرز المبادرات المهنية للأمن السيبراني في السعودية؟

اسم المعلم /ة:

٢

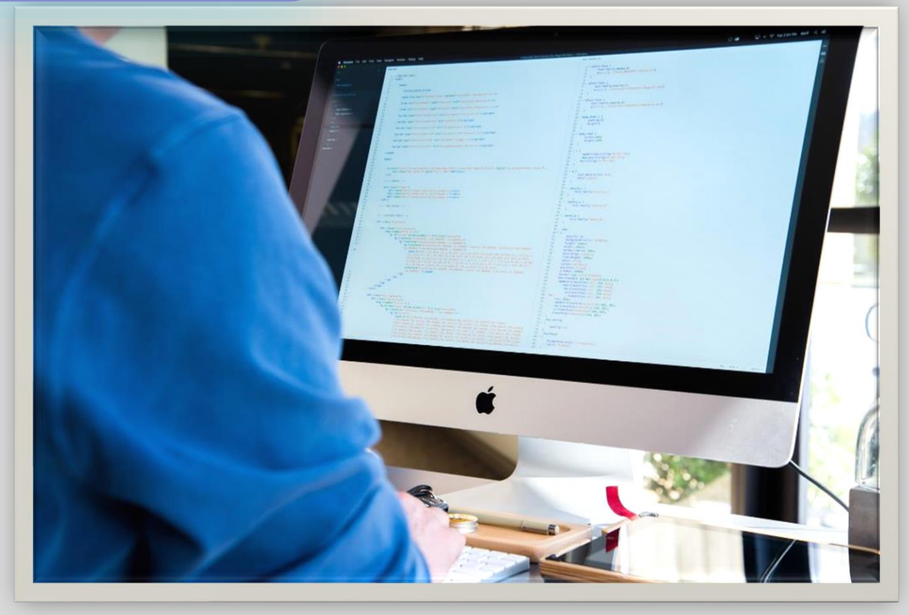
الأمن السيبراني ١٤٤٧ هـ

وزارة التعليم

# ورقة العمل

# عرض محتوى الكتاب

## الأدوار الوظيفية في الأمن السيبراني



يقدم مجال الأمن السيبراني مجموعة واسعة من فرص العمل للأفراد ذوي الخلفيات والمهارات المختلفة، حيث تتنوع هذه الفرص بين الأدوار التقنية مثل : محللي الأمن السيبراني،وأخصائيي اختبار الاختراقات، والأدوار الإدارية مثل : رئيس إدارة الأمن السيبراني (Chief Information Security Officer - CISO) ، وهناك مجموعة متنوعة من الأدوار الوظيفية في الأمن السيبراني تناسب الرغبات المختلفة والأهداف المهنية، بالإضافة إلى الأدوار الفنية والادارية، هناك أيضا فرص عمل خاصة بسياسات وحوكمة الأمن السيبراني مثل : مستشاري الأمن السيبراني وأخصائيي الالتزام في الامن السيبراني ، حيث أدى العجز الكبير في متخصصي الامن السيبراني محليا وعالميا إلى جعل هذا المجال من أكثر المجالات الوظيفية المستقبلية المطلوبة وأهمها ، وفيما يلي بيان للأدوار الوظيفية الرئيسية في الأمن السيبراني كما وردت في الاطار السعودي لكوادر الأمن

# عرض محتوى الكتاب

## دور حكومة المملكة العربية السعودية في الأمن السيبراني

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. نظرًا للنطاق الواسع للتطبيقات المختلفة في الأمن السيبراني، والتي تشمل الصناعات والقطاعات المختلفة، يتم تقييم مستوى

# عرض محتوى الكتاب

**عدد أبرز المبادرات المهنية للأمن السيبراني في المملكة العربية السعودية.**

التعليم والتدريب

استراتيجية الأمن السيبراني

الشراكات الصناعية

تطوير قطاع الأمن السيبراني

15صفحة:

# مهارة التفكير

وزارة التعليم


لماذا كل هذا الاهتمام في الأمن السيبراني؟

# النشاط الصفي

تدريب: 7 صفحة: 19

**تدريب ٧**

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

# ماذا تعلمنا خلال الدرس ؟

- ما الأدوار الوظيفية في الأمن السيبراني؟
- ما الدور المقدم من الحكومة السعودية نحو الأمن السيبراني؟
- ما أبرز المبادرات المهنية للأمن السيبراني في السعودية؟

الاسم: ..... الصف: .....

**السؤال الأول: ضع علامة ( ✓ ) أمام العبارة الصحيحة وعلامة ( × ) أمام العبارة الخاطئة:**

| | | |
|---|---|---|
| ١. | تم تطوير جدران الحماية والتشفير لمكافحة الهجمات السيبرانية المتزايدة. | ☐ |
| ٢. | تعد الوكالات الحكومية من الأهداف الرئيسية للهجمات السيبرانية. | ☐ |
| ٣. | ليست جميع الجرائم الإلكترونية لها نفس المستوى من الخطورة والعواقب. | ☐ |
| ٤. | السرية والسلامة والمصادقة تُشكل مثلث أمن المعلومات. | ☐ |
| ٥. | الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز هو مؤسسة وطنية تهدف إلى تدريب المواهب المحلية في مجال الذكاء الاصطناعي. | ☐ |
| ٦. | تشير السلامة إلى التأكد من دقة البيانات وعدم التلاعب بها. | ☐ |
| ٧. | يُعتبر التشفير والتحكم في الوصول وإخفاء البيانات من الطرق المستخدمة للحفاظ على سرية البيانات. | ☐ |
| ٨. | تضمن السرية أن البيانات دقيقة ولم يتم التلاعب بها. | ☐ |
| ٩. | رئيس إدارة الأمن السيبراني (CISO) مسؤولًا تنفيذيًا يشرف على برنامج الأمن السيبراني لمؤسسة معينة. | ☐ |
| ١٠. | رئيس إدارة الأمن السيبراني يؤدي دورًا وظيفيًا في مجال الأمان السيبراني. | ☐ |



# الواجب المنزلي

للمجموعة

التقويم النهائي

وزارة التعليم

# مشروع الوحدة الأولى

صفحة رقم 48

## الطرح والمناقشة

- تعريف الطلبة بالمشروع وخطواته.
- عرض فكرة المشروع وأهدافه المرتبطة بالوحدة.
- توضيح خطوات التنفيذ ومعايير التقييم.
- تقسيم الطلبة إلى مجموعات أو تكليف فردي
- تحديد زمن التنفيذ وجدول المتابعة وموعد التسليم.

خلال عملك كموظف في شركة مالية كبيرة، تم تكليفك بإنشاء تحليل أمني شامل لمجلس إدارة الشركة، حيث ستعرِض التهديدات من البرمجيات الضارة و الهجمات السيبرانية المتقدِّمة وكيف يُمكن لاستراتيجيات إدارة المخاطر مساعدة الشركة في التخفيف من تأثيرها، وستقوم بتحليل التهديدات التي تواجهها الشركات مثل شركتك، و الخطوات التي يُمكن اتخاذها لتأمين أنظمة المعلومات الخاصة بها.

1. عرِّف البرمجيات الضارة و الهجمات السيبرانية المتقدِّمة و اعرِض أمثلة عليها، ثم اشرح عواقب الهجمات الضارة على نظام معلومات الشركة.

2. حدِّد عمليات تحديد المخاطر وقيّمها، ثم صِفْ الاستراتيجيات المختلفة التي يُمكن استخدامها لتقليل المخاطر المرتبطة بالبرمجيات الضارة و الهجمات السيبرانية المتقدِّمة.

3. ركِّز على أهمية إدارة المخاطر المستمرة و المراقبة في مجال الأمن السيبراني، و اعرض دراسات حالة لمؤسسات تمكنت بشكل فعَّال من إدارة المخاطر التي تشكلها البرمجيات الضارة و الهجمات السيبرانية المتقدِّمة.

4. أنشئ عرضًا تقديميًا باستخدام **باوربوينت** (PowerPoint) من أجل تقديمه لمجلس إدارة الشركة، بحيث يتضمن الملاحظات المذكورة أعلاه، ويوجز ضرورة استراتيجيات الأمن السيبراني الفعَّالة و أهميتها في العصر الرقمي.


# همسات

## توعوية

وزارة التعليم

# من خلال العنوان الدرس

## مقدمة في الأمن السيبراني

نقوم بتعبئة الخانتين على اليسار

| ماذا أعرف ؟ | ماذا أريد أن أعرف ؟ | ماذا تعلمت ؟ | كيف أتعلم المزيد ؟ |
| --- | --- | --- | --- |
| | | | |


# ختام
# الدرس