وزارة التعليم

الوحدة الأولى الدرس الأول

الأمن السيبراني

من مقرر ثالث متوسط

الفصل الدراسي الأول ١٤٤٧ هـ

وزارة التعليم

بيانات الدرس

رقم الدرس

الدرس الأول

عنوان الدرس

مقدمة في الأمن السيبراني

عدد الحصص

حصتان

صفحات الكتاب

الحصة الأولى

من صفحة: 13

إلى صفحة: 16

وزارة التعليم

من خلال العنوان الدرس

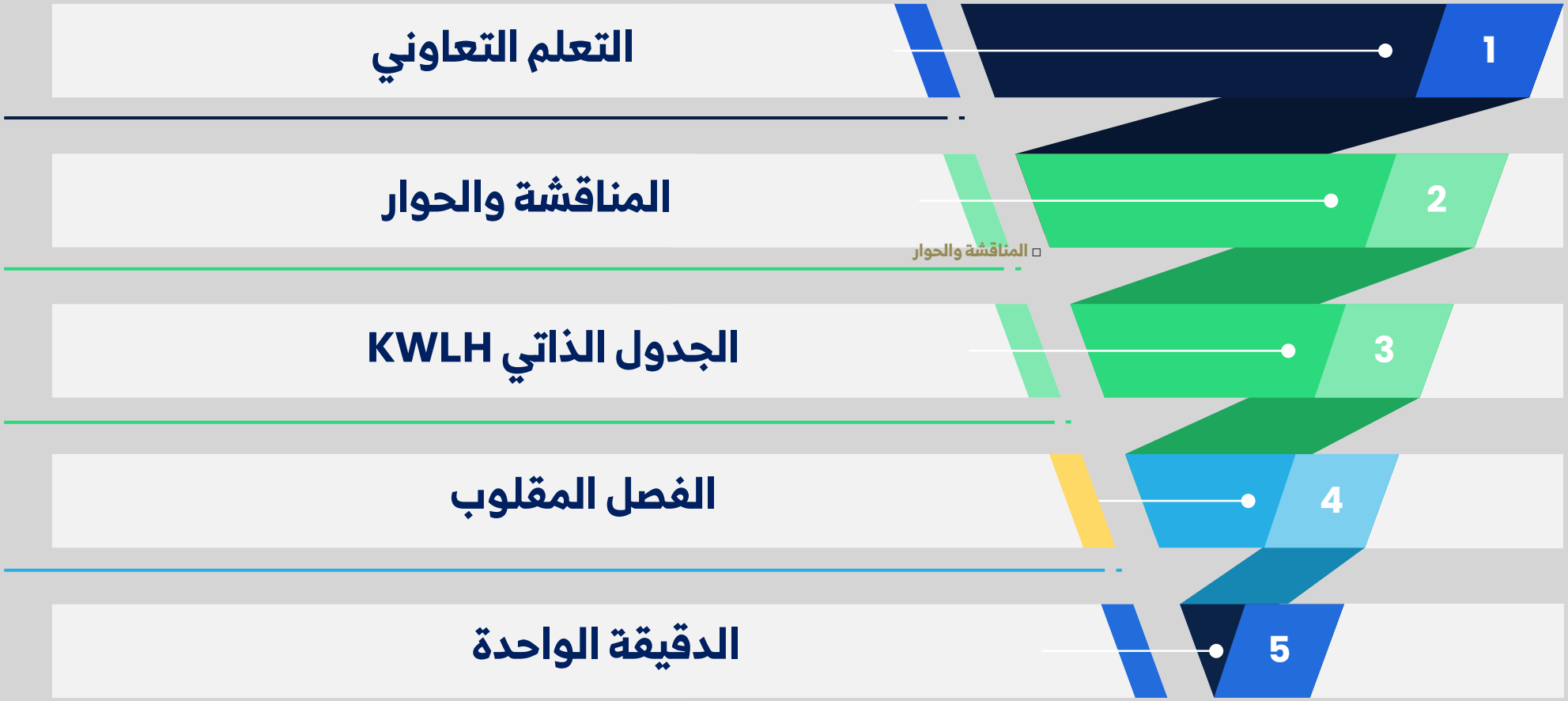
مقدمة في الأمن السيبراني

نقوم بتعبئة الخانتين على اليمين

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

وزارة التعليم

الإستراتيجيات



وزارة التعليم

تمهيد الدرس

الوحدة الأولى/ الدرس الأول

مقدمة في الأمن السيبراني

- ماذا نعني بمفهوم الأمن السيبراني؟
- هل سبق أن سمعتم بتعرض أحد لاختراق حساباته في مواقع التواصل الاجتماعي؟
- ما المقصود بالجرائم الإلكترونية؟ من هم الأفراد أو الكيانات المتورطة فيه؟
- مَن منكم يستخدم التحقق الثنائي لحماية حساباته على الإنترنت؟
- هل قمت بتفعيل التحقق الثنائي في منصة مدرستي؟

مغامرة نورة

استيقظت نورة لتجد نفسها داخل مدينة رقمية تُدعى "سيبرون"، حيث البيانات تمشي والمعلومات تتحدث! عند مدخل المدينة، رحب بها الحارس الآلي قائلاً:
- مرحبًا بكِ في عالم الأمن السيبراني! لتدخلي بأمان، عليكِ فهم سر مثلث الحماية:) CIAالسرية، التكامل، التوافر).

واصلت نورة سيرها، وسمعت عن الهجمات السيبرانية مثل التصيد والفيروسات، ورأت لوحات تحذر من الجرائم الإلكترونية مثل سرقة الهوية والاحتيال المالي.

في إحدى الساحات، شاهدت كيف يؤدي الإهمال الأمني إلى تسرب البيانات، وتعلمت أن خطأ صغير قد يسبب ضررًا كبيرًا.

في النهاية، قدّم لها روبوت وقائي درعًا وقال:
- استخدمي كلمات مرور قوية، ولا تضغطي على الروابط المشبوهة، وكوني دائمًا واعية رقميًا.

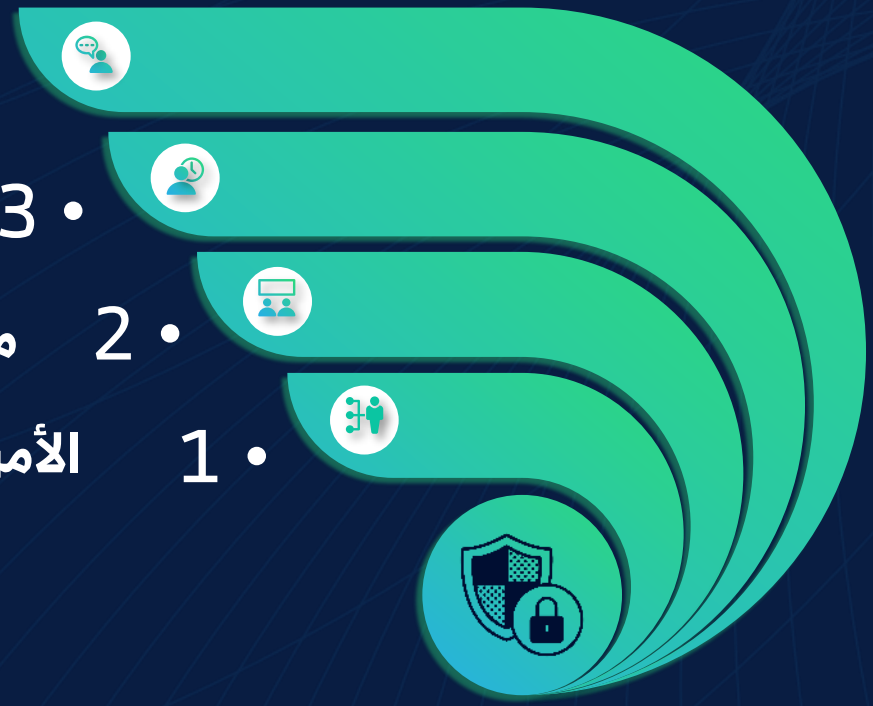
ابتسمت نورة، وعادت لعالمها، وهي تعرف جيدًا أهمية الأمن السيبراني في حماية الجميع.

النشاط الإثرائي

وزارة التعليم

مفردات الدرس

- 4 الاختراق الأمني
- 3 الجرائم الإلكترونية
- 2 مثلث الحماية CIA
- 1 الأمن السيبراني



وزارة التعليم

ماذا سنتعلم ؟

- الأمن السيبراني.
- أهمية الأمن السيبراني.
- مثلث الحماية CIA.
- الجرائم الإلكترونية.
- أنواع الجرائم الإلكترونية.
- ماهية الاختراق الأمني.

وزارة التعليم

ربط بالوطن

في المملكة العربية السعودية، تسعى الهيئة الوطنية للأمن السيبراني إلى تعزيز الأمان السيبراني من خلال برنامج "سايبر"، الذي يركز على حماية البيانات الحكومية والشخصية من التهديدات الإلكترونية. يتضمن البرنامج تنفيذ استراتيجيات متقدمة مثل مراقبة الشبكات وتحليل التهديدات، وتدريب موظفي الحكومة على أفضل ممارسات الأمن السيبراني، لضمان سلامة المعلومات الحساسة وحماية الثقة في الأنظمة الرقمية من خلال الاستجابة الفعّالة للهجمات الإلكترونية.

وزارة التعليم

ورقة العمل

عرض محتوى الكتاب

الأمن السيبراني:

يتعلق مفهوم الأمن السيبراني بحماية أجهزة الحاسب والشبكات والبرامج والبيانات من الوصول غير المصرح به، والذي قد يهدف إلى الحصول على المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال، بل وأحيانًا تعطيل عمليات المؤسسة عمومًا. يُعبِّر مصطلح الأمن السيبراني عن جميع الممارسات التي تتم لحماية المعلومات من المخاطر والهجمات التي تتمثل في الوصول غير المصرح به بغرض الاستخدام غير المشروع أو التعديل أو الإتلاف أو النسخ غير المصرح به أو تزوير المعلومات.

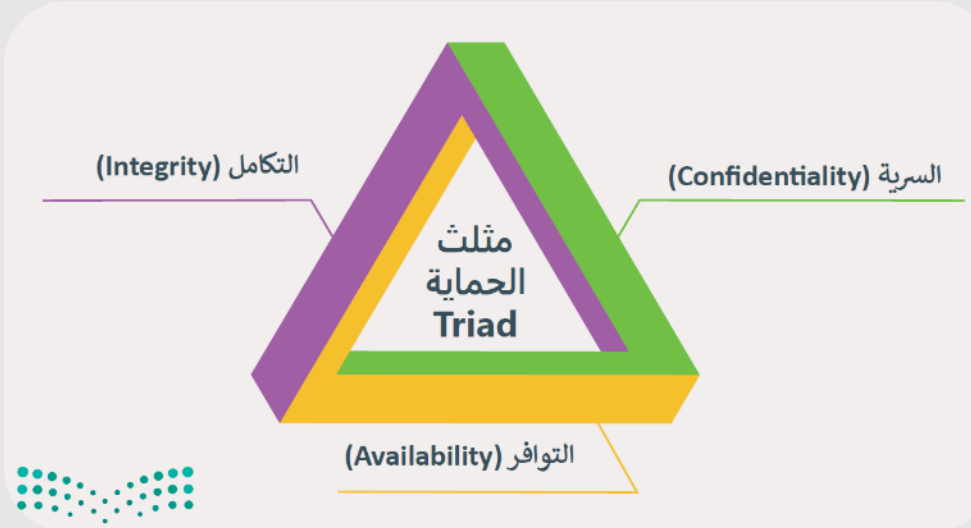
عرض محتوى الكتاب

أهمية الأمن السيبراني:

تزداد أهمية الأمن السيبراني بزيادة أهمية البيانات والمعلومات المتوفرة على الشبكة، وضرورة توافرها للمستخدمين دون انقطاع، بالإضافة إلى عدد المستخدمين الذين يحتاجون للوصول إلى تلك البيانات والمعلومات بشكل مستمر، وكلما زادت أهمية المعلومات كلما كانت عرضة لهجمات القرصنة الحاسوبية بهدف سرقتها أو حجبها عن المستخدمين وغير ذلك. يتمثل الدور المهم للأمن السيبراني في منع التهديدات الداخلية والخارجية واكتشافها والقيام بالاستجابة المناسبة لها حسب الضرورة.

عرض محتوى الكتاب

مثلث الحماية CIA:



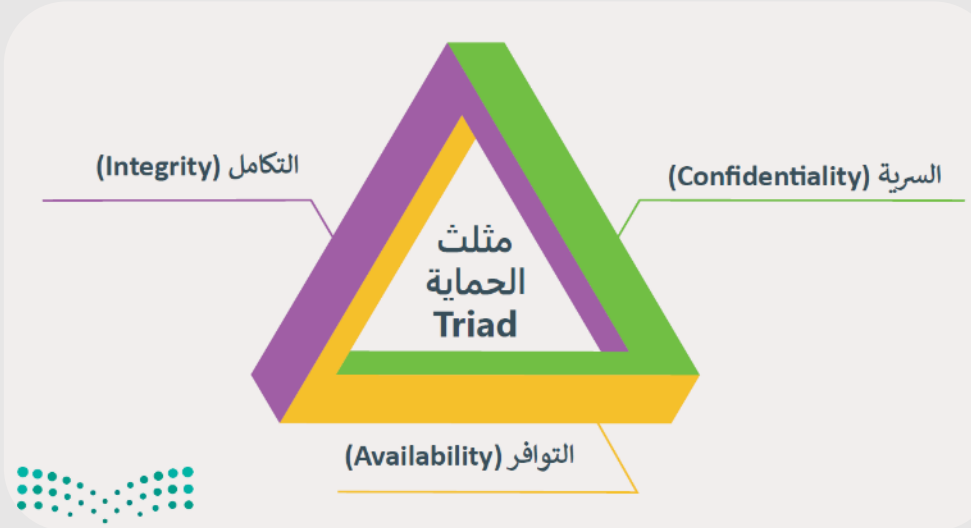
01 **السـرية:** السـرية هـي إتاحـة البيانـات والمعلومـات للأشـخاص المعنيين بها فقط والمسموح لهم بالاطلاع عليها، ولتحقيق ذلك يتم استخدام أساليب مختلفة مثل اسم المستخدم وكلمة المرور، وقوائم الأشخاص ذوي الصلاحيات.

02 **التكامل:** يشير مصطلح التكامل إلى الحفاظ على دقة وصحة المعلومات، والتأكد من عدم إمكانية تعديلها إلا من قبل الأشخاص المخولين بذلك، ومن أساليب الحفاظ على تكامل البيانات والمعلومات: تحديد الأذونات والصاحيات، والتشفير، وغيرها.

عرض محتوى الكتاب

مثلث الحماية CIA:

03 **التوافر:** التوافر يعني ضمان الوصول للمعلومات في الوقت المناسب وبطريقة موثوقة لاستخدامها، حيث إن أي نظام معلومات عليه توفير المعلومات عند الحاجة إليها وذلك ليؤدي الغرض الأساسي له.
ومن أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات، الحفاظ على سلامة الأجهزة المستضيفة للبيانات، والنسخ الاحتياطي، وتحديثات النظام، وتحسين كفاءة الشبكة لتسهيل وصول المستخدمين ما أمكن.



عرض محتوى الكتاب

الجرائم الإلكترونية:

أنواع الجرائم الإلكترونية:

01 **الاحتيال الإلكتروني:** يحدث هذا الاحتيال عندما يتقمص المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية، بغرض الحصول على معلومات شخصية عن مستخدم معين مثل كلمات المرور المصرفية وعنوان البيت أو الرقم الشخصي. تتم هذه العملية عادةً من خلال مواقع الاحتيال التي تُقلد المواقع الرسمية.

02 **سرقة الهوية**: بعد سرقة البيانات الشخصية، يقوم المحتالون بانتحال شخصية الضحية واستخدام بياناته لإجراء معاملات مالية، أو أعمال غير قانونية.

عرض محتوى الكتاب

الجرائم الإلكترونية:

أنواع الجرائم الإلكترونية:

03 **المضايقات عبر الإنترنت:** تشمل التهديدات عبر البريد الإلكتروني أو الرسائل الفورية أو المشاركات المسيئة في وسائل التواصل الاجتماعي مثل فيسبوك وتويتر.

04 **التسلل الإلكتروني:** عادة ما يصيب المتسللون الإلكترونيون أجهزة الحاسب الخاصة بضحاياهم ببرامج ضارة يمكنها تسجيل نشاط الحاسب لمراقبة نشاطاتهم عبر الإنترنت، فمثلا يقوم برنامج مسجل المفاتيح بتتبع وتسجيل أزرار لوحة المفاتيح المضغوطة بطريقة سرية بحيث يصعب على الشخص معرفة أنه تتم مراقبته وجمع بياناته الخاصة.

عرض محتوى الكتاب

الجرائم الإلكترونية:

أنواع الجرائم الإلكترونية:

05 **انتهاك الخصوصية:** يحدث انتهاك الخصوصية عند محاولة شخص ما التطفل على الحياة الشخصية لشخص آخر، وقد يتضمن ذلك اختراق الحاسب الشخصي الخاص به أو قراءة رسائل البريد الإلكتروني أو مراقبة الأنشطة الشخصية الخاصة به عبر الإنترنت.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:

01 **فيسبوك:** في عام 2019 ، كشف باحثوا أمن المعلومات أن ملايين سجلات مستخدمي فيسبوك كانت منتشرة عبر الإنترنت، بسبب قيام بعض التطبيقات التي يسمح لها فيسبوك بالوصول إلى بيانات مستخدميه بتخزين تلك البيانات على خوادم خاصة بها دون وضع تدابير الأمان المطلوبة، وتم العثور على ملايين السجلات بما فيها معرفات المستخدمين على فيسبوك، التعليقات، الإعجابات، ردود الفعل وأسماء الحسابات في قاعدة بيانات تم تحميلها بواسطة الناشر الرقمي المكسيكي كولتورا كوليكتيفا الذي تم اكتشافه على الخوادم السحابية لخدمات أمازون ويب، وهذا يدعو إلى اتخاذ تدابير الحيطة والحذر قبل السماح لبرامج الأطراف الخارجية التي تصادفنا على منصات التواصل الاجتماعي بالوصول إلى معلوماتنا.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:

02 **ماريوت الدولية:** في نوفمبر 2018 ، سرق لصوص الإنترنت بيانات ما يقارب 500 مليون عميل لشركة ماريوت الدولية، وتعتقد الشركة أن أرقام بطاقات الائتمان وتواريخ انتهاء الصلاحية لأكثر من 100 مليون عميل قد سُرقت أيضًا، رغم أنه لم يكن من المؤكد فيما إذا تمكن المهاجمون من فك تشفير أرقام بطاقات الائتمان.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:

03 **جوجل+:** في أكتوبر 2018 ، تم الإبلاغ عن اختراق مبدئي طال 500 ألف من مستخدمي جوجل+، ولكن شركة جوجل أعلنت عن الاختراق بعد عدة أشهر من اكتشافه. في ديسمبر، كشفت الشركة عن اختراق أخر للبيانات تم خلاله كشف المعلومات الشخصية ل 52,5. مليون حساب على جوجل+ لمدة ستة أيام لتطبيقات غير جوجل+. تضمن هذا الاختراق بيانات مثل الأسماء، عناوين البريد الإلكتروني، تواريخ الميلاد ونوع المعلومات الشخصية الأخرى التي تم جمعها بواسطة جوجل+.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:

04 **تويتر:** في عام 2019 ، قام مئات من مستخدمي تويتر عن غير قصد بإعطاء بياناتهم الشخصية لتطبيقات طرف ثالث. اعترفت الشركة بأنها أصدرت إصلاحًا لرمز خبيث ربما تم إدراجه في تطبيقها من قِبل قراصنة الحاسب وكان من الممكن أن يعرض معلومات بعض المستخدمين في جميع أنحاء العالم للخطر. تم إعلام شركة تويتر بالمشكلة من قِبل باحثي أمن تابعين لجهة ثالثة، اكتشفوا أن مجموعات تطوير برامج وان أودينس وموبي بيرن قد سمحت بالوصول إلى بيانات المستخدمين الحساسة. شملت المعلومات المكشوفة أسماء المستخدمين، عناوين البريد الإلكتروني والتغريدات الحديثة.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:

05 **أدوبـي:** أعلنـت الشـركة فـي البدايـة بـأن المتسـللين سـرقوا مـا يقـارب 3 ملايـين مـن سـجلات بطاقـات ائتمـان العمـلاء المشـفرة، بالإضـافة إلـى بيانـات تسـجيل الـدخول لعدد غير محدد من حسابات المستخدمين، ولكن بعد أسابيع من البحث تم اكتشاف أن هذا الاختراق قد كشف عن الكثير مـن بيانـات العمـلاء بمـا فيهـا مُعرِّفـاتهم وكلمـات المـرور ومعلومات بطاقات الخصم وبطاقات الائتمان الخاصة بهم.

وزارة التعليم

مهارة التفكير

هل تطوير الأمن السيبراني مهم للحكومة؟ وضح ذلك؟

وزارة التعليم

النشاط الصفي

تدريب: 4 صفحة: 21

تدريب ٤

❖ اشرح ما الاختراق الأمني. بعد ذلك، اكتب قائمة بالإجراءات التي يمكنك اتخاذها لحماية نفسك من الانتهاكات الأمنية.

وزارة التعليم

ماذا تعلمنا خلال الدرس ؟

1. ما المقصود بالأمن السيبراني؟
2. ما أهمية الأمن السيبراني؟
3. ما مكونات مثلث الحماية CIA؟ مع الشرح؟
4. ما المقصود بالجرائم الإلكترونية؟
5. ما أنواع الجرائم الإلكترونية؟
6. ما خطورة الاختراق الأمني؟ مع الأمثلة؟

وزارة التعليم

الواجب المنزلي

للمجموعة

تدريب: 2 صفحة: 20

تدريب ٢

❖ وضح بالشرح العناصر التي يتكون منها مثلث الحماية CIA، ثم وضح كيفية تطبيق هذا النموذج على أنظمة الصراف الآلي ATM.

وزارة التعليم

ختام الحصة الأولى

وزارة التعليم

بيانات الدرس

رقم الدرس

الدرس الأول

عنوان الدرس

مقدمة في الأمن السيبراني

عدد الحصص

حصتان

صفحات الكتاب

الحصة الثانية

من صفحة: 17

إلى صفحة: 20

وزارة التعليم

الواجب المنزلي

للمجموعة

تدريب: 2 صفحة: 20

تدريب ٢

❖ وضح بالشرح العناصر التي يتكون منها مثلث الحماية CIA، ثم وضح كيفية تطبيق هذا النموذج على أنظمة الصراف الآلي ATM.

العناصر التي يتكون منها نموذج مثلث الحماية CIA هي: السرية (Confidentiality)، التكامل (Integrity)، التوافر (Availability).

لتطبيق هذا النموذج على أنظمة الصراف الآلي ATM، يمكن اتخاذ الإجراءات الآتية:

(1) السرية: يمكن تحقيق السرية من خلال تنفيذ آليات مصادقة قوية، مثل: رموز PIN، والحد من الوصول المادي إلى أجهزة الصراف الآلي، وتشفير قنوات الاتصال بين أجهزة الصراف الآلي وشبكة البنك.

(2) التكامل: لضمان تكامُل أنظمة الصراف الآلي ATM، يجب إجراء تحديثات منتظمة للبرامج، كما يجب تثبيت برامج مكافحة الفيروسات وبرامج مكافحة البرمجيات الضارة وصيانتها. بالإضافة إلى ذلك، يمكن تنفيذ تدابير الأمن المادي مثل كاميرات المراقبة، وغيرها.

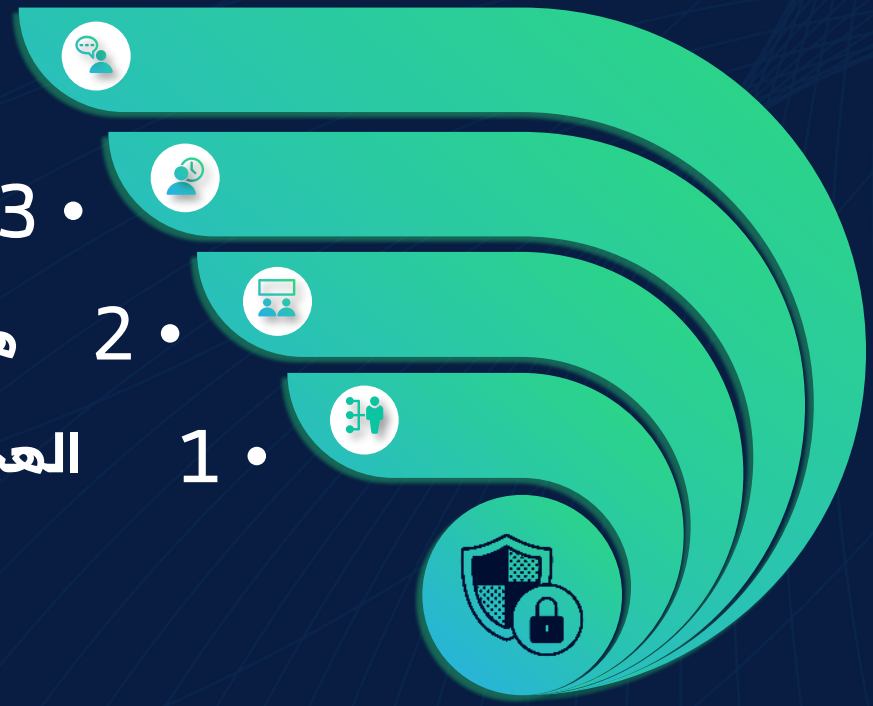
(3) التوافر: لضمان توافر أنظمة الصراف الآلي ATM، يمكن استخدام مكونات الأجهزة والبرامج المتكررة، ويجب إجراء الصيانة والمراقبة المستمرة لاكتشاف المشكلات وحلها قبل أن تؤدي إلى توقُّف العمل. كما يجب أيضًا إنشاء نسخ احتياطية من بيانات العملاء وتخزينها بانتظام في مواقع آمنة.

النشاط الإثرائي

وزارة التعليم

مفردات الدرس

- 4 الوقاية من الجرائم الإلكترونية
- 3 هجوم الوسيط
- 2 هجمات حجب الخدمات
- 1 الهجمات الإلكترونية



وزارة التعليم

ماذا سنتعلم ؟

- الهجمات الإلكترونية.
- مقارنة بين هجمات حجب الخدمات وحجب الخدمات الموزع.
- هجوم الوسيط.
- أمثلة على الوسيط الإلكتروني.
- طرق الوقاية من الجرائم الإلكترونية.

وزارة التعليم

ورقة العمل

عرض محتوى الكتاب

الهجمات الإلكترونية:

الهجمات الإلكترونية هي محاولات لسرقة المعلومات، أو كشفها، أو تعطيلها، أو إتلافها من خلال الوصول غير المصرح به إلى جهاز الحاسب. وهي أيضًا محاولة للوصول غير المصرح به إلى نظام الحوسبة أو شبكة الحاسب بقصد إحداث ضرر. عادة ما يتم تنفيذ الهجمات الإلكترونية بطريقة غير قانونية وبنية إحداث ضرر، ويمكن أن يكون لها عواقب وخيمة على المهاجمين.

عرض محتوى الكتاب

هجمات حجب الخدمات وحجب الخدمات الموزع:

01 **هجوم حجب الخدمات:** هجوم حجب الخدمات هو نوع من أنواع الهجمات السيبرانية حيث يقوم جهاز حاسب واحد أو شبكة بإغراق موقع أو خادم مستهدف بحركة المرور، مما يؤدي إلى إرباكه وجعله غير متاح للمستخدمين.

02 **هجوم حجب الخدمات الموزع:** هجوم حجب الخدمات الموزع هو إصدار أكثر تقدمًا من هجوم حجب الخدمات حيث يتم استخدام العديد من أجهزة الحاسب أو الشبكات لإغراق موقع ويب أو خادم مستهدف بحركة المرور، مما يجعل الدفاع ضده أكثر صعوبة. تجعل المصادر المتعددة لحركة المرور من الصعب منع الهجوم؛ لأنه يبدو أنه قادم من مواقع متعددة.

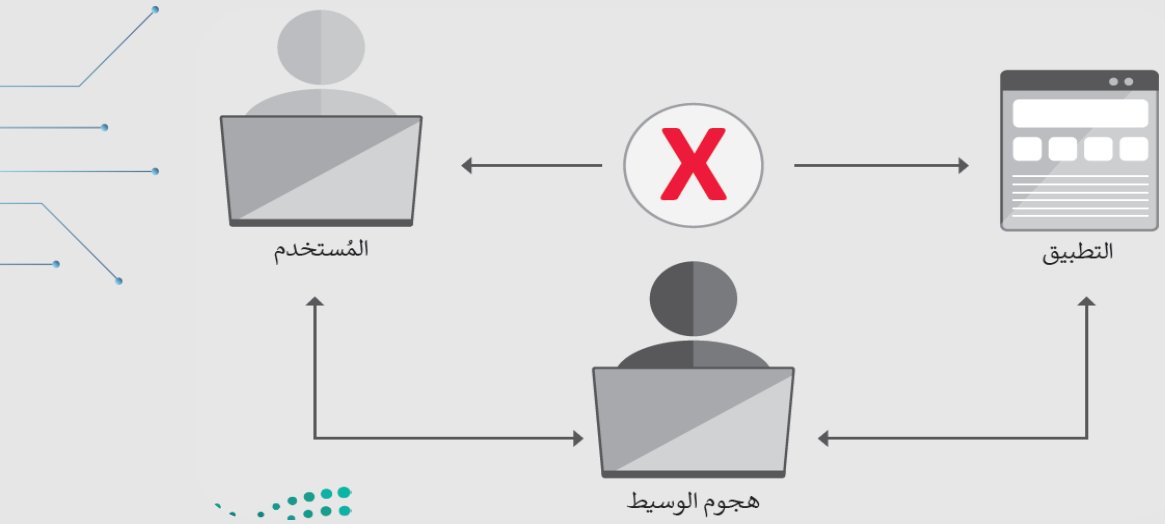
عرض محتوى الكتاب

هجمات حجب الخدمات وحجب الخدمات الموزع:

03 **هجوم الوسيط:** هجوم الوسيط هو نوع من الهجمات الإلكترونية يتطفل فيه المهاجم بين اتصال المستخدم والتطبيق، ويجلس في منتصفه متظاهرًا بأنه الطرف الآخر، ويمكنه قراءة أو تعديل أو إدخال رسائل جديدة في تدفق الاتصال. يمكن استخدام هجوم الوسيط لسرقة معلومات حساسة أو نشر برامج ضارة أو تنفيذ أنشطة ضارة أخرى. يمكن التخفيف من هذه الهجمات باستخدام أساليب التشفير والمصادقة.

عرض محتوى الكتاب

هجمات حجب الخدمات وحجب الخدمات الموزع:



أمثلة على هجوم الوسيط الإلكتروني:

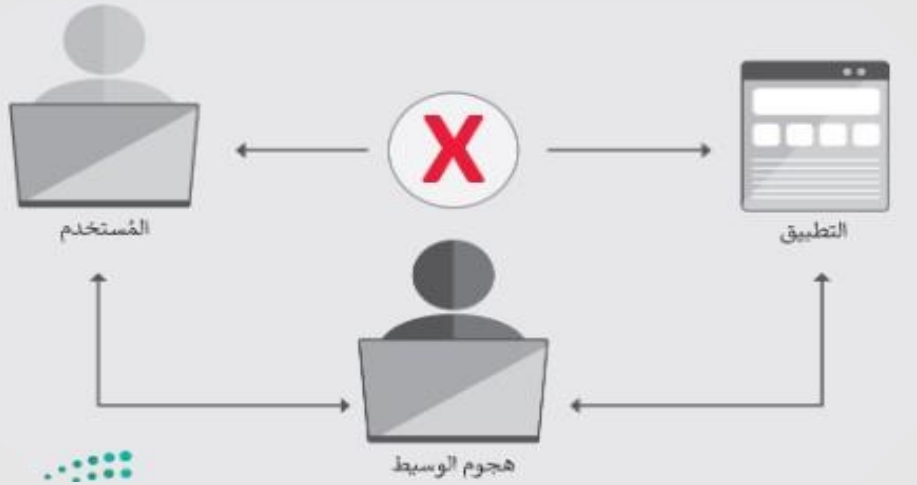
01 **التنصت على الواي فاي:** يمكن للمهاجم إعداد نقطة وصول واي فاي خادعة تظهر على أنها نقطة وصول شرعية، مما يسمح له باعتراض وقراءة حركة مرور الشبكة غير المشفرة المرسلة من قبل الضحايا المطمئنين الذين يتصلون بنقطة الوصول الخادعة.

02 **انتحال أسماء النطاقات:** في هذا الهجوم، يعترض المهاجم استعلامات نظام اسم النطاق DNS ويغيرها، ويعيد توجيه الضحايا إلى موقع ويب ضار بدلًا من موقع الويب المشروع المقصود.

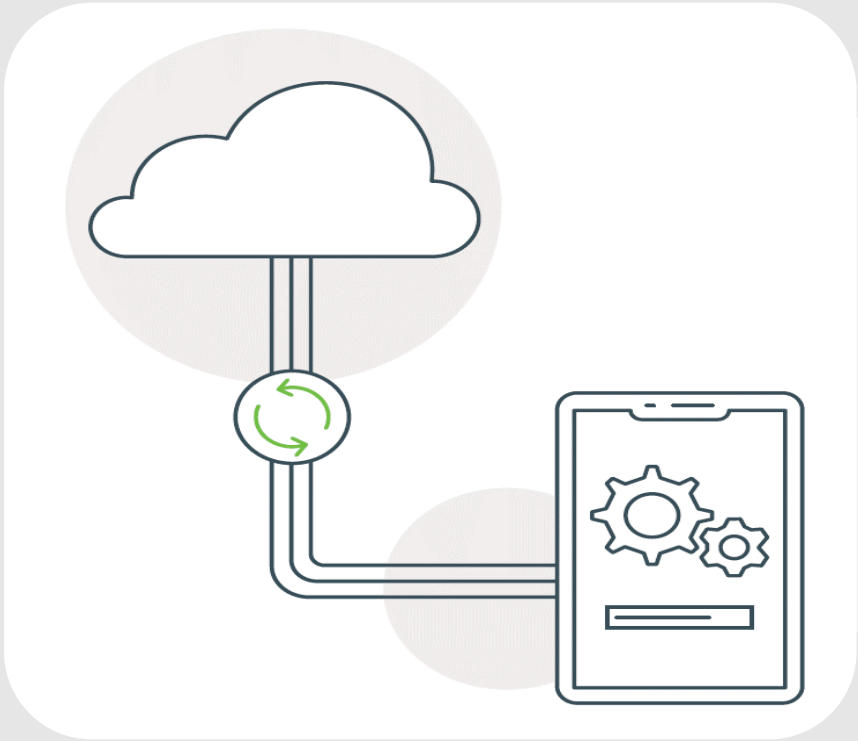
عرض محتوى الكتاب

أمثلة على هجوم الوسيط الإلكتروني:

03 **التصيد الاحتيالي للبريد الإلكتروني:** في هذا النوع من الهجوم يعترض المهاجم رسائل البريد الإلكتروني وتغيير المحتوى أو إضافة مرفقات أو روابط ضارة لسرقة معلومات حساسة أو لنشر برامج ضارة.



عرض محتوى الكتاب

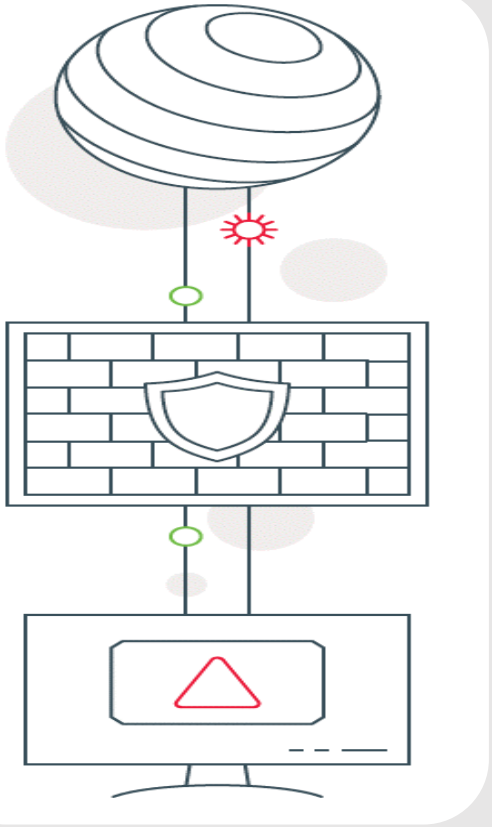


الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

01 **التحديث الدوري للبرامج:** يُعدُّ تحديث البرمجيات أحد أكثر حلول الأمن السيبراني للتقليل من خطر برمجيات الاختراق الخاصة وخاصة تلك التي تعتمد على ابتزاز المستخدم، يجب أن يشمل هذا التحديث المستمر كلًا من نظام التشغيل والتطبيقات، وذلك لإزالة الثغرات الأمنية الحرجة التي قد يستخدمها المتسللون للوصول إلى الأجهزة الثابتة والمحمولة والهواتف الذكية.

عرض محتوى الكتاب



الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

02 **استخدام برامج مكافحة الفيروسات وجدار الحماية:** يُعدُّ برنامج مكافحة الفيروسات الحل الأكثر نجاحًا في محاربة الهجمات؛ نظرًا لأنه يمنع البرمجيات الضارة والفيروسات الخبيثة الأخرى من الدخول إلى جهازك وتعريض بياناتك للخطر، ويُعدُّ استخدام برنامج حماية مناسب مهمًا في الحفاظ على بياناتك من الهجمات، فهو يساعد على حجب المتسللين والفيروسات والنشاطات الضارة الأخرى عبر الإنترنت وتحديد وتقنين البيانات المسموح بمرورها إلى جهازك.

يتحكم جدار الحماية في حركة مرور البيانات الواردة والصادرة من خلال تحليل حزم البيانات وتحديد ما إذ اكان ينبغي السماح بمرورها أم لا. وقد تأتي جدر الحماية على صورة برامج يتم تثبيتها على أجهزة الحاسب بشكل فردي، أو على شكل أجهزة خارجية منفصلة تستخدم ضمن هيكل الشبكة لحمايتها من الهجمات الخارجية. يمكن لبرامج جدار الحماية المثبتة على أجهزة الحاسب الفردية أن تفحص البيانات عن كثب، ويمكن أن تمنع برامج محددة من إرسال البيانات إلى الإنترنت. تستخدم الشبكات ذات الاحتياطات الأمنية العالية كلا النوعين من جدران الحماية لتأمين شبكة أمان كاملة.

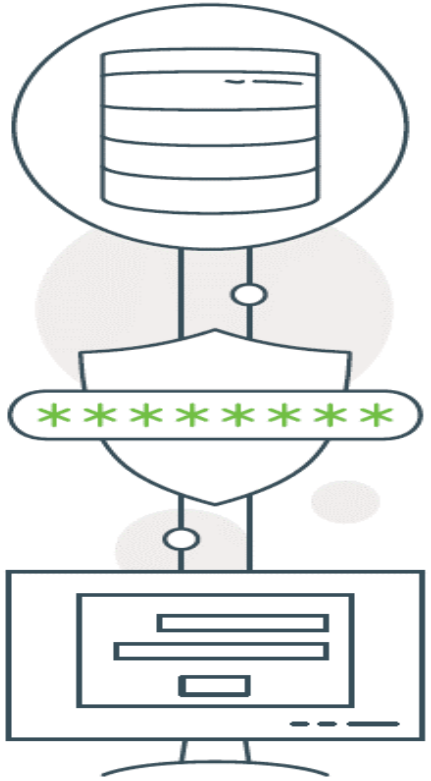
عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

03 **التواصل الرقمي الحذر:** الانتباه إلى كافة أشكال التواصل الرقمي سواء عبر البريد الإلكتروني أو منصات التواصل الاجتماعية وحتى المكالمات الهاتفية والرسائل النصية. فمثلًا تجنب فتح الرسائل الإلكترونية المرسلة من جهات مجهولة، والتأكد من الروابط التشعبية بدقة قبل الضغط عليها، وتوخي الحذر من مشاركة أي معلومات شخصية عبر هذه المنصات.

عرض محتوى الكتاب



الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

04 **استخدام كلات المرور القوية وأدوات كلمات المرور:** يُعدُّ استخدام كلمات المرور القوية أمرًا ضروريًا مهمًّا لاعتبارات الأمن عبر الإنترنت، ووفقًا لسياسة استخدام كلمات المرور الجديدة، يجب أن تكون كلمة المرور القوية على درجة كافية من التعقيد، وتتغير بشكل دوري. وفي هذا الوقت الذي تتعدد حسابات المستخدمين على منصات وتطبيقات عديدة، ظهرت الحاجة إلى استخدام أدوات إدارة كلمات المرور والتي تحتفظ بكلمات المرور بصورة مشفرة في قواعد بيانات آمنة، بحيث يتم استرجاعها عند طلب المستخدم والتحقق من هويته.

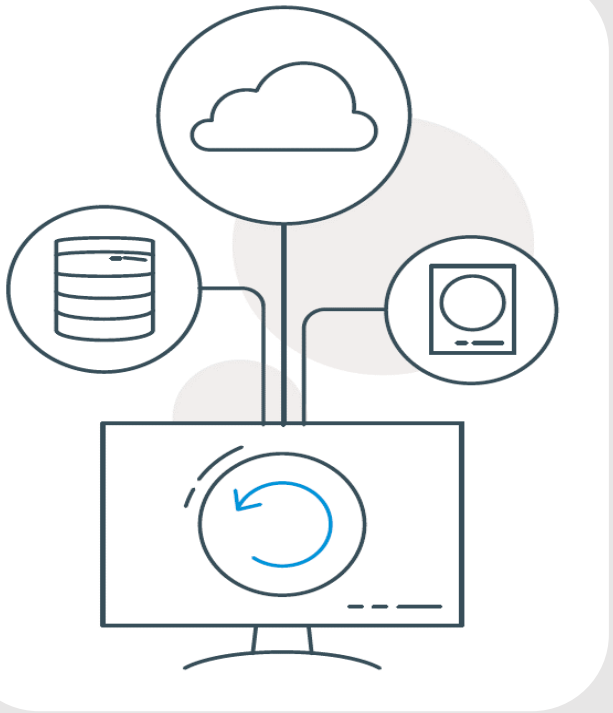
عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

05 **التحقق الثنائي أو المتعدد:** تقدم عملية التحقق الثنائي أو المتعدد خيارات أمان إضافية، حيث تتطلب عملية المصادقة التقليدية إدخال اسم المستخدم وكلمة المرور فقط، بينما يتطلب التحقق الثنائي استخدام طريقة إضافية كرمز التعريف الشخصي أو كلمة مرور أخرى أو حتى استخدام بصمة الإصبع. أما استخدام التحقق متعدد العوامل فيتطلب أكثر من طريقتين. تتضمن أمثلة التحقق الثنائي أو المتعدد استخدام مزيج من هذه العناصر للمصادقة مثل: الرموز الناتجة عن تطبيقات الهواتف الذكية، البطاقات أو أجهزة USB أو الأجهزة المادية الأخرى، بصمات الأصابع، الرموز المرسلة إلى عنوان بريد إلكتروني، التعرف على الوجه وإجابات لأسئلة الأمان الشخصي.

عرض محتوى الكتاب



الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

06 **النسخ الاحتياطي الدوري للبيانات:** يعد إجراء نسخ احتياطي للبيانات بشكل دوري خطوة مهمة في مجال الحفاظ على أمان الإنترنت الشخصي، فبشكل أساسي عليك الاحتفاظ بثلاث نسخ من بياناتك على نوعين مختلفين من وسائط تخزين البيانات، كنسختين على (القرص الصلب المحلي والخارجي)، ونسخة أخرى على موقع خارجي أو باستخدام التخزين السحابي. في حالة استهدافك بالبرمجيات الضارة تكون الطريقة الوحيدة لاستعادة البيانات هي باستعادة آخر نسخة احتياطية كبديل عن النظام الحالي المصاب بالبرمجيات الضارة.

عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

07 **تجنب استخدام شبكات واي فاي العامة:** ينصح بتجنب استخدام شبكة واي فاي العامة دون استخدام شبكة افتراضية خاصة، فباستخدام هذه الشبكة، يتم تشفير حركة نقل البيانات بين الجهاز وخادم VPN مما يصعب على القراصنة الوصول إلى بياناتك على الإنترنت، كما يوصى باستخدام الشبكة الخلوية عند عدم وجود شبكة VPN وذلك للحصول على مستوى أعلى من الأمان.

وزارة التعليم

مهارة التفكير

لماذا تنشط الهجمات الإلكترونية وقت الحروب؟

وزارة التعليم

النشاط الصفي

تدريب: 5 صفحة: 22

تدريب ٥

اختر الإجابة الصحيحة:		
1. إتاحة البيانات والمعلومات للأشخاص المعنيين بها فقط والسماح لهم بالاطلاع عليها هو مفهوم:	السرية.	○
	التكامل.	○
	التوافر.	○
	التنوع.	○
2. من أساليب الحفاظ على تكامل البيانات والمعلومات:	النسخ الاحتياطي.	○
	تحديثات النظام.	○
	اسم المستخدم وكلمة المرور.	○
	الأذونات والصلاحيات.	○
3. التهديدات عبر البريد الإلكتروني أو الرسائل الفورية أو المشاركات المسيئة عبر وسائل التواصل الاجتماعي هو مفهوم:	الاحتيال الإلكتروني.	○
	التسلل الإلكتروني.	○
	المضايقات عبر الإنترنت.	○
	انتهاك الخصوصية.	○

وزارة التعليم

ماذا تعلمنا خلال الدرس ؟

1. ما المقصود بالهجمات الإلكترونية؟
2. ما الفرق بين هجوم حجب الخدمات وهجوم حجب الخدمات الموزع؟
3. ما المقصود بهجوم الوسيط؟
4. ما الأمثلة على هجوم الوسيط الإلكتروني؟
5. ما طرق الوقاية من الجرائم الإلكترونية؟

وزارة التعليم

الواجب المنزلي

للمجموعة

التقويم النهائي

الاسم: ..... الصف: .....

ضع علامة(✓) أمام الإجابة الصحيحة:

١	**المقصود بالأمن السيبراني:**	
أ	حماية الأجهزة من التلف	☐
ب	حماية الأجهزة والبيانات من الوصول غير المصرح به	☐
ج	تحسين أداء الحاسب وحماية الحاسب من الفيروسات القوية	☐
د	تثبيت البرامج الجديدة والمفيدة	☐
٢	**الأهداف الرئيسية للأمن السيبراني:**	
أ	حماية المعلومات الحساسة من الوصول غير المصرح به	☐
ب	الحفاظ على سلامة البيانات ومنع تعديلها أو إتلافها	☐
ج	ضمان توافر المعلومات عند الحاجة	☐
د	جميع ما ذكر	☐
٣	**ماذا قد يحدث في حالة عدم وجود أمن سيبراني؟**	
أ	الوصول غير المصرح به للمعلومات	☐
ب	تغيير المعلومات أو إتلافها	☐
ج	تعطيل عمليات المؤسسة	☐
د	جميع ما ذكر	☐
٤	**الدور المهم للأمن السيبراني:**	
أ	منع التهديدات الداخلية فقط	☐
ب	منع التهديدات الخارجية فقط	☐
ج	منع التهديدات واكتشافها والاستجابة المناسبة حسب الضرورة	☐
د	حماية الأجهزة من التلف	☐

وزارة التعليم

مشروع الوحدة الأولى

صفحة رقم: 41

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.

بالتعاون مع مجموعة من زملائك في الصف، وبالبحث في المواقع الموثوقة؛ قدم عرضًا تقديميًا حول أحد الموضوعات الآتية:

الأمن السيبراني ونصائح للبقاء آمنًا عند الاتصال بالإنترنت، ويمكنك زيارة موقع العطاء الرقمي https://attaa.sa. وتصفح مكتبة الموقع الإلكتروني، وتصفح سلسلة فيديو بودكاست تسمى سايبر إكس، للبحث عن معلومات حول الأمن السيبراني. ستجد معلومات مفيدة حول مخطط المعلومات المرفق في المقالة، صمم عرضك التقديمي مع تسليط الضوء على الخطوات البسيطة التي يمكن لشخص ما أن يتخذها للبقاء آمنًا عند الاتصال بالإنترنت.

التنمر الإلكتروني وطرق تجنبه، ويمكنك زيارة الموقع الإلكتروني https://thinktech.sa. وتصفح موضوعات المدونة المتاحة. ومن قسم الفعاليات اختر موضوع التنمر الإلكتروني وتعزيز الصحة النفسية، وشاهد مقاطع الفيديو المتوفرة، واجمع المعلومات المناسبة لموضوع بحثك وقدمها في عرضك التقديمي مع نصائح لزملائك حول كيفية مواجهتها والحماية منها.

الجرائم الإلكترونية وكيفية الحماية منها، ويمكنك زيارة موقع الهيئة الوطنية للأمن السيبراني https://www.nca.gov.sa. للبحث عن معلومات حول الجريمة الإلكترونية وأمثلة محتملة لها. وعن النموذج الذي يمكنك استخدامه للإبلاغ عن الجرائم الإلكترونية، وأضفها في العرض التقديمي الخاص بك، وقدم نصائح لزملائك للحماية من هذه الجرائم والابلاغ عنها عند التعرض لها.

صمم عرضك التقديمي مع مراعاة الجوانب الجمالية عند التصميم، وإضافة الصورة المناسبة لموضوع بحثك، وتوثيق مصادرك.

قدم عرضك وناقش زملاءك في الصف حول المعلومات الواردة فيه، ثم عدله بناء على نتائج المناقشة وارفعه لمعلمك عبر البريد الإلكتروني.

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 ؟

وزارة التعليم

ختام الدرس