الجرائم السيبرانية، وجهود مكافحتها محليًا ودوليًا

وصف الدرس:

الهدف العام من الدرس أن ينمّي الطالب وعيه بخطورة الجرائم السيبرانية، والتعرف على ماهيتها، وتصنيف أنشطتها، والإبلاغ عنها حال وقوعها، ويتعرّف على الجهود المحلية والدولية في مكافحة الجرائم السيبرانية، كما ينمّي وعيه بأهمية الالتزام بقانون مكافحة الجرائم المعلوماتية السعودي، ويوعّي المجتمع تبعًا لذلك.

أهداف التعلم:

1. أن يتعرف الطالب على الجريمة السيبرانية، وأركانها، والفرق بين مصطلحاتها.
2. أن يشارك الطالب بوضع حلول لعوائق مكافحة الجرائم السيبرانية.
3. أن يناقش الطالب دوافع ارتكاب الجريمة السيبرانية، وآثارها على الحكومات والشركات.
4. أن يصنّف الطالب الجرائم السيبرانية الشائعة في شبكة الإنترنت.
5. أن يمارس الطالب إجراءات التبليغ عن الجريمة السيبرانية حال وقوعها.
6. أن يعرف الطالب أهمية الجهود المحلية والعالمية في مكافحة الجرائم السيبرانية.
7. أن يثمن الطالب جهود المملكة العربية السعودية في مكافحة جرائم المعلوماتية.
8. أن يشارك الطالب المجتمع حول الأضرار التي تسببها الجرائم السيبرانية.
9. أن يصنّف الطالب الجرائم السيبرانية بحسب عقوباتها في قانون مكافحة جرائم المعلوماتية السعودي.
10. أن ينشر الطالب توعية في المجتمع بأهمية قانون مكافحة جرائم المعلوماتية.

إرشادات للمعلم قبل الدرس:

- تقسّم أهداف الدرس إلى ثلاث حصص دراسية.
- الاطلاع والبحث عن مفهوم الجرائم السيبرانية، وأنّ استيعابك لهذا المفهوم وأنشطته المنتشرة دوليًا يجعلك متمكنًا في درسك.
- البحث عن أحد الفيروسات المشهورة التي كان لها حدث بارز عالميًا، ومعرفة آثاره التي تسبب بها، والدور الذي قام به المتضررون لأجل إصلاح آثاره.
- تنبيه الطلبة بالاطلاع على نظام مكافحة جرائم المعلوماتية السعودي قبل حضورهم الحصة الدراسية لأخذ فكرة عن النظام ومواده، واستيعابه مما يسّهل عليهم التفاعل أثناء الحصة الدراسية، وتوجيههم بالبحث عنه بواسطة مسح رمز الاستجابة في الدرس، أو عبر محرك البحث، أو بإرسال الرابط لهم عبر مدونة المادة، أو عبر البريد الإلكتروني أو بأي وسيلة متبعة في المقرر.
- يمتلك الطلبة في مرحلة الصف الثالث الثانوي غالبًا جهاز هاتف محمول، وقد يحضرونه للمدرسة، وقد يعرفون أو لا يعرفون بوجود عقوبات على مخالفة التصوير بالجوال في غير موضعه، وقد يجهلون بوجود قانون لمكافحة جرائم المعلوماتية في المملكة العربية السعودية.

- بيّن للطلاب أن لكل دولة قانونها الخاص الذي يختلف في مواده عن الدولة الأخرى في عقوبة السجن أو المخالفة المالية.
- يفضّل عرض قانون مكافحة جرائم المعلوماتية أمام الطلبة في الدرس لأجل حل الأنشطة والتدريبات، وكذلك لاستعراض المواد الأخرى غير المذكورة في الدرس.
- التنويع في الدرس ما بين معرفي ومهاري واتجاهات وقيم، لذلك يجب أن يكون الطالب مشاركًا فاعلًا في عملية التعلُّم، وفاعلًا في أنشطة الدرس، ومطالبته بالاطلاع على الدرس قبل حضوره للصف الدراسي، وتنفيذ المهام أثناء الدرس وبعده.


الدرس الأول

الجرائم السيبرانية
وجهود مكافحتها محليًا ودوليًا

رابط الدرس الرقمي
www.ien.edu.sa

مخرجات التعلم:

- أتعرّف على الجريمة السيبرانية، وأركانها، والفرق بين مصطلحاتها.
- أشارك في وضع حلول لعوائق مكافحة الجرائم السيبرانية.
- أناقش دوافع ارتكاب الجريمة السيبرانية، وآثارها على الحكومات والشركات.
- أصنّف الجرائم السيبرانية الشائعة عبر شبكة الإنترنت.
- أبلغ عن الجريمة السيبرانية حال وقوعها.
- أتعرف على أهمية الجهود العربية والعالمية في مكافحة الجرائم السيبرانية.
- أثمّن جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية.
- أشارك مجتمعي حول الأضرار التي تسببها الجرائم السيبرانية.
- أربط الجرائم السيبرانية بعقوباتها في نظام مكافحة جرائم المعلوماتية السعودي.
- أنشر توعية بأهمية نظام مكافحة جرائم المعلوماتية لأفراد المجتمع.

مصطلحات الدرس:

- الجريمة السيبرانية (CyberCrime).
- المخترقون (Hackers).

التهيئة

- هل لديك فكرة عن الأضرار التي أحدثتها بعض الفايروسات الحاسوبية المشهورة كسلامر (Slammer)، ولوف (ILOVEYOU)، وساسر (Sasser) من تعطّل للأجهزة، وتشفير للملفات، ومدى تأثيرها المادي والمعنوي؟
- ماذا لو تعرّض مزود خدمة الإنترنت بالمملكة العربية السعودية إلى هجوم سيبراني أدى لتوقفه، ما الضرر الناتج الذي سيحدث للخدمات الإلكترونية الحكومية، التعاملات التجارية، الأسواق المالية، تعاملات الأفراد اليومية؟
- هل تعتقد أن المجرمين السيبرانيين يعملون في الخفاء ولا يمكن كشفهم؟
- لماذا يلجأ المجرمون السيبرانيون لمحاولة الكسب السريع عبر الأعمال الإجرامية بدلًا من ممارسة العمل السليم؟
- هل سمعت عن خبر لمخالفة معلوماتية في إحدى وسائل الإعلام الرقمية؟ وما رأيك في تصرّف صاحبها؟
- هل تفكّر قبل إجراء أي عمل أثناء استخدامك شبكة الإنترنت ما إذا كان نافعًا أم ضارًا لك أو لغيرك؟
- هل تشعر بالندم لتصرف مارسته سابقًا أثناء استخدامك لشبكة الإنترنت؟ وكيف تداركت الموقف في وقتها؟

162

التمهيد في بداية الدرس:

- ابدأ الدرس بسؤال الطلبة عن مدى معرفتهم بمفهوم الجرائم السيبرانية، واعمل عصفًا ذهنيًّا لإجاباتهم على السبورة كمقدمة للدرس.
- اذكر مثالًا على إحدى الجرائم السيبرانية المشهورة لتقريب المثال للطالب قبل الدخول في تعريفات الدرس.
- زود الطلبة بتعريف - التعريفات للاستئناس بها ولا يُلزم الطلبة بها- معنى الجريمة وهي: (إتيان فعل أو تركه عن إرادة جنائية إضرارًا بمصلحة اجتماعية حماها المشرع بقواعد تجرمه وتعاقب عليه جزائيًا)، كما يُعرّف الإرهاب حسب تعريف قانون مكافحة الإرهاب السعودي الصادر عام (2013م) بأنه: (كل فعل يقوم به الجاني تنفيذًا لمشروع إجرامي فردي أو جماعي بشكل مباشر أو غير مباشر، يقصد به الإخلال بالنظام العام، أو زعزعة أمن المجتمع واستقرار الدولة أو تعريض وحدتها الوطنية للخطر، أو تعطيل النظام الأساسي للحكم أو بعض مواده، أو الإساءة إلى سمعة الدولة أو مكانتها، أو إلحاق الضرر بأحد مرافق الدولة أو مواردها الطبيعية، أو محاولة إرغام إحدى سلطاتها على القيام بعمل ما أو الامتناع عنه، أو التهديد بتنفيذ أعمال تؤدي إلى المقاصد المذكورة أو التحريض عليها).
- استعرض أسئلة التمهيد الموجودة في كتاب الطالب.
- في موضوع نظام مكافحة الجرائم المعلوماتية السعودي احصِ الطلبة الذين بحثوا واطّلعوا على النظام لعمل ربط بينه وبين الأفكار التالية:
  - بيّن للطلاب أهمية أن يكون هناك قوانين في أي دولة تحكم الممارسات والتعاملات داخلها، ويجب على المواطن احترامها وعدم مخالفتها؛ وذلك لينعم المواطنين في رخاء ونظام، ولعدم التعرض لأي عقوبات.
  - اذكر أمثلة على قوانين موجودة يحترمها الطالب في عمره، مثل لائحة المخالفات السلوكية في المدرسة، وبيّن لماذا تعمل إدارة المدرسة بشكل سنوي على إطلاع الطلبة للائحة وتوقيعهم عليها.
  - في الحصة الثالثة من الدرس استرجع تعريف (الجريمة، والجريمة السيبرانية) في الحصة الأولى لهذه الوحدة؛ وذلك لعمل ربط بين موضوعات الدرس، ولاسترجاع المعلومة من قِبل الطلبة للبناء عليها.

إجراءات تنفيذ الدرس:

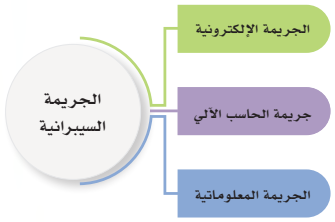
- يُستعرض مفهوم الجريمة السيبرانية، والفرق بينه وبين المصطلحات الأخرى التي تتكرر عبر شبكة الإنترنت، والإشارة إلى أنها متشابهة ولا يوجد فرق بينها، وأن الاختلاف فقط يكون في المسمى، لكن الاختلاف يكون بين الجهات التي سعت في البداية لإيجاد مفهوم لتفسير هذه الظاهرة.
- ناقش الطلبة عن هذه المفاهيم، وأيها يرون أنه مناسب أو أقرب للظاهرة الحالية، يمكن وضع تصويت (Rank) على السبورة، أو استخدام تصويت رقمي تفاعلي بين الطلبة (كأداة كاهوت Kahoot، أو قوقل فورم Google Form على سبيل المثال).
- محاولة استثارة عقول الطلبة حول (إثارة التفكير: هل يوجد فرق بين مرتكب الجريمة السيبرانية، ومرتكب الإرهاب الإلكتروني من حيث النظام؟).
- توضح هنا أركان الجريمة السيبرانية، وتوجيه الطلبة إلى أن الجريمة قد لا تكون بمحض الصدفة، وإنما هي عمل منسّق، ومنظم، ويتم فيه الإعداد وتجهيز الأدوات المادية والبرمجية التي تحقق الجريمة، وأن المجرمين السيبرانيين نوعان: هواة ومحترفون.
- يطلب من الطلبة في النشاط (3-1) استنباط الدوافع التي يلجأ لها المجرمون السيبرانيون من خلال استيعاب أركان الجريمة، ومحاولة استخلاص الدوافع منها ومن خلال موضوع (مفهوم الجريمة السيبرانية).

الجريمة السيبرانية والمصطلحات المرتبطة بها

أدى تطور الجريمة ووصولها إلى أجهزة الحاسوب المتصلة بشبكة الإنترنت إلى ظهور مفاهيم عدة في الأدبيات والقوانين الدولية تصف العمل الإجرامي الإلكتروني، فبرزت مصطلحات: الجريمة السيبرانية، الجريمة المعلوماتية، جريمة الحاسب الآلي، الجريمة الإلكترونية، الإرهاب الإلكتروني شكل (3-1)، إلا أن أكثرها تداولًا في المنظمات الدولية هي الجريمة السيبرانية (CyberCrime) التي تعرف بأنها: (نشاط إجرامي يستهدف أو يستخدم جهاز حاسوب أو شبكة حاسوبية أو جهازًا متصلًا بالشبكة بواسطة مجرمي الإنترنت)، وتهدف هذه الجريمة إلى كسب المال، أو إتلاف الممتلكات المادية والبرمجية، أو لأسباب أخرى قد تكون سياسية أو عسكرية أو شخصية.

شكل (3-1): مصطلحات الجرائم السيبرانية

يتوافق مفهوم (الجريمة السيبرانية) كثيرًا مع مصطلحات (الجريمة الإلكترونية)، (الجريمة المعلوماتية)، (جريمة الحاسب الآلي) كونها جميعًا تعبّر عن أي فعل إجرامي مشين يتم باستخدام الأجهزة والأنظمة الرقمية، فلا فرق يُذكر بينهم، بينما يُقصد بمصطلح (الإرهاب الإلكتروني) ممارسة أفعال الإرهاب من عنف أو تخويف أو تهديد لأمن الدول أو الأفراد باستخدام الأجهزة والأنظمة الرقمية والشبكية بأنواعها، ومن ثمّ يُعد متقاربًا مع المصطلحات الأخرى في حال كون الموضوع يتعلق بالاعتداءات التي تكون ضمن محيط الحاسوب سواء كانت مادية أو معنوية.



شكل (3-2): توافق مصطلحات الجرائم السيبرانية

إثارة التفكير:

هل يوجد فرق بين مرتكب الجريمة السيبرانية ومرتكب الإرهاب الإلكتروني من حيث النظام؟

أركان الجريمة السيبرانية

توجد عدة أركان للجريمة السيبرانية، ويختلف تصنيفها بناءً على ظروف ارتكاب الجريمة السيبرانية، أو دوافعها، أو الأدوات المستخدمة بها، إلا أنه يمكن إيجاز أركان الجريمة السيبرانية فيما يأتي:

أولًا: مرتكب الجريمة السيبرانية: هو الشخص المنفذ للجريمة، ويُعد الطرف الأهم والأخطر بسبب كونه المتسبب الرئيس في ارتكاب العمل الإجرامي، وينقسم المجرمين المنفذين حسب دوافعهم إلى نوعين:

النوع الأول	النوع الثاني
الأفراد الفضوليون الذين يتطفلون على الآخرين، ويحاولون الوصول لبياناتهم، أو أسرارهم الشخصية ككلمة المرور لحساباتهم، أو صورهم الشخصية وخلافه، لغرض الاستمتاع، أو التحدي، أو إثبات النفس أمام الآخرين بامتلاك الخبرة في هذا المجال.	المخترقون (الهكرز Hackers)، وهم مجموعة من الأشخاص متخصصون في الاختراق، ويتواصلون مع بعضهم افتراضيًا من دول مختلفة لتبادل الخبرات، والتعاون فيما بينهم لتنفيذ ممارساتهم إما لأهداف سياسية أو عسكرية بالإضافة للانتفاع المالي الذي يعد الهدف الأساسي.

ثانيًا: الأجزاء المادية: هي الأجهزة والأدوات المستخدمة لفعل السلوك الإجرامي كأجهزة الحاسوب الثابتة والمتنقلة بأنواعها، وأدوات الاتصال الشبكي، وكل جهاز يستخدم في الجريمة، كما تشمل الأدوات البرمجية كالبرامج، والتطبيقات، ومواقع شبكة الإنترنت، وكل ما اتصف بصفة رقمية.

ثالثًا: السلوك الجرمي: هو الفعل والنشاط الذي يقوم به المجرم السيبراني عبر استخدام الأجزاء المادية والبرمجية للوصول إلى الهدف المراد.

نشاط فردي 1-3

بالعودة لأركان الجريمة السيبرانية، استنبط دوافع ارتكاب الجرائم السيبرانية من قبل المجرمين السيبرانيين؟

.....

.....

.....

.....

- توجد هنا قائمة بأنشطة الجريمة السيبرانية في جدول (3-1)، والتي جُمعت من عدة مصادر عبر شبكة الإنترنت، تُعرض للطالب ويُناقش بمدى خطورتها، وذكر أمثلة لاستخداماتها، وتوجيه الطالب بحل تدريبي (3-1) و (3-2) بناءً على استيعابه لأنشطة الجرائم السيبرانية مباشرة.
- تخصص (5) دقائق لكل تدريب كحد أقصى.

أنشطة الجرائم السيبرانية

تشترك معظم أنظمة مكافحة الجرائم السيبرانية الدولية في تصنيف أنشطة الجرائم السيبرانية المشهورة عالميًا،ويمكن استعراضها في الجدول (3-1) الآتي:

جدول (3-1): أنشطة الجرائم السيبرانية

1	التزوير باستخدام الحاسوب.	2	الاحتيال باستخدام الحاسوب.
3	إتلاف الأجهزة أو البرامج أو الشبكات الحاسوبية.	4	الوصول غير المشروع إلى البيانات المخزنة، واستغلالها وتسريبها وإعادة استخدامها بغير وجه حق.
5	التنصت والتجسس على أنشطة الحاسوب أو البيانات أو الاتصالات.	6	استخدام البرامج المحمية بدون تصريح أو التعديل عليها أو إلغاء حمايتها.
7	الاتجار بالبشر، واستغلال الأطفال.	8	الاعتداء على حقوق الطبع والمؤلف كالكتب والأدبيات والمقاطع المرئية والتسجيلات الصوتية.
9	الاتجار بالأسلحة النارية والمخدرات وممارسة غسل الأموال عبر شبكة الإنترنت.	10	اقتحام الأنظمة والشبكات وانتهاك سلامتها أو تعطيلها.
11	ممارسة الأفعال غير الأخلاقية عبر شبكة الإنترنت، وتناقل المواد المحظورة شرعيًا ونشرها كالصور ومقاطع الفيديو.	12	سرقة الأموال والبطاقات البنكية الائتمانية.
13	إنتاج ونشر مواد معادية للدين الإسلامي وأمن الوطن.	14	التعدي على الخصوصية من خلال سرقة الهوية والتصوير واستغلال المعلومات الشخصية للاستفادة منها.

تدريب 1-3

بنـاء على اطلاعك على قائمة الأنشـطة الإجرامية في جـدول (3-1)، صنّف الممارسـات الإجرامية عبر تحديد نوع النشاط الإجرامي لكل ممارسة في الجدول الآتي:

م	الممارسة الإجرامية	النشاط الإجرامي التابع له
1	إرسال ملف للآخرين لمعرفة ما لديهم من معلومات.	
2	إنشاء موقع إلكتروني وهمي لبيع المستلزمات الطبية.	
3	مطاردة شخص عبر شبكة الإنترنت ومضايقته وتهديده.	
4	الدخول غير المصرح لموقع فندق وحجز غرفة.	
5	فك حماية برنامج لغرض العمل عليه.	
6	إنشاء صفحة تسجيل دورة تدريبية لاختبار القدرات لسرقة الأموال.	
7	إرسال رسالة احتيالية للبريد الإلكتروني من شركة شحن دولية.	
8	التسلل إلى إحدى خوادم شركات الاتصالات لحذف الفواتير المخزنة للمشتركين.	
9	الحصول على ملف معلومات مهمة لمناقصة تجارية لإحدى الشركات.	
10	إرسال ملف للآخرين لتشفير ملفاتهم وطلب مبلغ مقابل فك التشفير.	
11	تعطيل نظام الإشارات المرورية.	
12	إرسال صور غير أخلاقية عبر إحدى وسائل التواصل الاجتماعي.	
13	تصوير الآخرين بكاميرا الهاتف النقال بدون علمهم.	
14	استخدام البطاقة البنكية لصديق من أجل الاشتراك بلعبة متصلة بالإنترنت.	
15	إجراء توقيع مزيف لتوقيع مسؤول على إحدى الفواتير الإلكترونية.	

تدريب 2-3

بيّن نوع الممارسات الرقمية من حيث انتمائها/عدم انتمائها لأنشطة الجرائم السيبرانية في الجدول الآتي:

م	الممارسة الإجرامية	انتماءها للجريمة السيبرانية	
		تنتمي	لا تنتمي
1	الوصول إلى جهاز خادم (server) بدون تصريح من الجهة المالكة.		
2	إنشاء موقع إنترنت لتقديم خدمة تصميم بنرات إعلانية.		
3	الشراء ببطاقة ائتمانية لشخص ما بدون إذنه.		
4	طلب بيانات شخصية من فرد عبر رسالة بالبريد الإلكتروني على شكل قالب تقديم وظيفة.		
5	الوصول لبيانات تسجيل الدخول لإحدى وسائل التواصل الاجتماعي من طرف ثالث من غير المستخدم والشبكة الاجتماعية نفسها.		
6	مساعدة الآخرين في مجال تعلّم البرمجة عبر مدونة خاصة.		
7	إنشاء موقع إنترنت لتقديم معلومات مضللة تهدف إلى تغيير الحقائق.		
8	وضع ملف تنصت داخل جهاز خادم (server) للحصول على بيانات المشتركين.		
9	بيع السلع غير المشروعة عبر شبكة الإنترنت.		
10	التغريد عبر تطبيق تويتر عن أخبار غير صحيحة.		

- وضّح للطالب العوائق التي تحول دون القضاء بشكل تام على الجرائم السيبرانية، واحرص على أن استيعاب الطالب لها بشكل واضح يمكّنه باقتراح حلول لهذه العوائق التي يمكن أن تختلف من طالب لآخر.
- في نشاط (3-2) أعطِ مجالًا لكل طالب بمحاولة اقتراح حل لهذه الجرائم بما لا يتجاوز (3) حلول، وأن يشارك النتيجة مع زملائه في الفصل، وفي حالة توفر أجهزة لدى الطلبة، (يمكن للطلاب مشاركة أعمالهم عبر أداة الحائط الإلكتروني (بادلت Padlet) -إن توفر ذلك-.
- في نشاط (3-3) قسّم الطلبة لمجموعات تعاونية، واجعلهم يقرأون القصة بتروّي وبمتابعة منك، واجعل طالبًا واحدًا يعمل على تسجيل ما يتوصلون له من إجابات فيما بينهم، أعطِ مجالًا لعرض الإجابات من المجموعات لكل سؤال من الأسئلة الخمسة. يفضّل تخصيص (10) دقائق لهذا النشاط.
- وضّح الجهود العربية والدولية في مكافحة الجريمة السيبرانية، وأنها آفة تصل لجميع الدول، وأنه لا يمكن أن يكون نطاق ضررها على دولة محددة في ظل ارتباط دول العالم بشبكة الإنترنت.
- يمكن توصية الطلبة بالبحث عن المنظمات المذكورة في الدرس لمعرفة الجهود المبذولة، والتأكيد على خطر الجرائم السيبرانية على الجميع، ويمكن تطبيق إستراتيجية البحث والاستقصاء.

عوائق مكافحة الجريمة السيبرانية

- تتم الجريمة السيبرانية بشكل خفي، بحيث لا يمكن في كثير من الأحوال صدها، أو تتبع أثرها إلا في نطاقات ضيقة أو بمحض الصدفة.
- تطور الجريمة المنظمة بحيث يجعل من الصعوبة اكتشافها، خصوصًا مع تطور الأنظمة التقنية والأجهزة والبرمجيات المستمر، ومع بطء تحديث قوانين مكافحة الجرائم السيبرانية.
- انتشار الجريمة السيبرانية على مستوى العالم، وعدم تحديدها بمنطقة معينة، فيمكن أن يكون مرتكبها في قارة، والجريمة المنفذة في قارة أخرى، مع صعوبة اقتفاء آثار مرتكبيها.
- قلة عدد المحققين في المجال الجنائي الرقمي، وقلة الخبرات في هذا المجال مقابل ازدياد عدد المجرمين السيبرانيين على مستوى العالم، وتواصلهم المستمر مع بعضهم البعض، ولهذا تظهر الحاجة إلى زيادة المتخصصين في مجال الأمن السيبراني.

شكل (3-3): عوائق مكافحة الجريمة السيبرانية

نشاط 2-3

اقترح حلولًا لعوائق مكافحة الجرائم السيبرانية التي درستها.

آثار الجريمة السيبرانية على الحكومات والشركات:

نشاط 3-3

اقرأ القصة الآتية:

تم اختراق شركة مشهورة عالميًا في عام 2014م، وبدأت الحادثة عندما تفاجأ الموظفون بإقفال شاشات أجهزتهم، وعدم قدرتهم على التحكم بها، وبعد ذلك أعلن بعض المخترقين عن أسمائهم السيبرانية، وأبدوا الأسباب التي دفعتهم لاختراق أنظمة الشركة شملت مطالبهم التي تم طلبها سابقًا من إدارة الشركة، وأظهروا الرسالة الآتية: (لقد استطعنا السيطرة على الشركة لأنها لم تغلق الأبواب جيدًا، وبالتعاون مع أحد موظفي الشركة)، وبعد عدة أيام، نشر المخترقون حسابات البريد الإلكتروني للموظفين، وبعض إنتاجات الشركة التي كلفت ملايين الدولارات، بعدها توالت نشر معلومات الشركة كرواتب الموظفين، وكلمات مرور أجهزتهم، وأرقام بطاقاتهم الائتمانية، وأرقام الضمان الاجتماعي لهم. الملفت للانتباه أن ملفات كلمات المرور المخزنة بداخل أجهزة الموظفين كانت مخزنة بدون حماية وبدون تشفير، وانتهت عملية التسريب بنشر أرقام بطاقات الائتمان لعملاء الشركة التي تم استخدامها لشراء منتجات الشركة.

الجهود العربية والدولية في مكافحة الجرائم السيبرانية

أقرت كثير من الدول العربية نظامها الخاص لمكافحة الجرائم السيبرانية، بدأتها المملكة العربية السعودية في إقرار قانون لمكافحة جرائم المعلوماتية، كما أقرّت عدة دول نظامها الخاص لاحقًا كالإمارات العربية المتحدة، والكويت، والمملكة الأردنية الهاشمية، وجمهورية مصر العربية، وغيرها من الدول. مع تسارع الدول العربية لإقرار قانونها الخاص؛ أسّست جامعة الدول العربية في عام2010م (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات)، وهدفت الاتفاقية على تعزيز التعاون بين الدول الأعضاء في مجال مكافحة جرائم المعلوماتية لدرء أخطارها، والحفاظ على مصالح الدول وأمنها، وسلامة مجتمعاتها وأفرادها.

على المستوى الدولي أقرّت كثيرًا من الدول العالمية قوانينها الخاص، ولتوحيد التنسيق بين الدول في مكافحة الجريمة السيبرانية؛ قامت الجهات والمنظمات الدولية بجهودٍ في هذا الجانب كما يتضح في الشكل (3-5) الآتي:

المجلس الأوروبي (European Council)
- تأسيس اتفاقية بشأن الجرائم المعلوماتية في بودابست- المجر بين دول القارة.
- تعد أول معاهدة دولية بشأن الجرائم التي تُرتكب عبر شبكة الإنترنت.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)
- تعاونَ المكتب مع الدول الأعضاء لدراسة الجريمة السيبرانية، والتصدي لها عبر تبادل التشريعات الوطنية، والمساعدة الفنية لأفضل الممارسات.

الشرطة الدولية (Interpol)
- ملاحقة المطلوبين بين الدول، وتقديم المعلومات المشتركة للقضاء عليهم.
- تحليل الجريمة السيبرانية، وطرائق تنفيذها لمنع تكرار وقوعها في ظروف مماثلة مستقبلًا.

شكل (3-5): الجهود الدولية في مكافحة الجرائم السيبرانية

- وضح جهود المملكة العربية السعودية في إنشاء الهيئات والأنظمة التي تكافح الجرائم السيبرانية، واضرب أمثلــة لاهتمام المملكة للوصول عالميًا في مصاف الدول التي تطبق الأمن الســيبراني في تعاملاتها وأنظمتها الرقمية.
- اجعل الطلبة يتذكرون المناسبات والأنشطة التي أقامتها الجهات الحكومية أو الخاصة في المملكة فيما يتعلق بالأمن السيبراني للتأكيد على توجه الدولة في تطبيق وإرساء معايير الأمن الرقمي بها.

جهود المملكة العربية السعودية في مكافحة الجريمة السيبرانية

اهتمت حكومة المملكة العربية الســعودية بالمحافظة على الأمن الســيبراني، والحماية من الجرائم الســيبرانية عبر إقرارهــا لقانون مكافحة الجرائــم المعلوماتية، حيث تولت هيئــة الاتصالات وتقنية المعلومات التصــدي لهذه المهمة، ثم تم إنشــاء الهيئة الوطنية للأمن الســيبراني في عام 1439هـ، وتُعنى هذه الهيئة بتنظيم إســتراتيجية الأمن السيبراني داخل الدولة، ووضع الآليات، والأطر، والمعايير، للجهات الحكومية، وغير الحكومية المتعلقة بالأمن السيبراني، وتحديثها باســتمرار، كما أنشــأت الهيئة مركزًا للتوعية والتنبيه بأخطار الأمن السيبراني من هجمات أو برمجيات ضارة أو اكتشاف ثغرات، وإشراك المجتمع للتعاون على مساعدتها لمواجهة هذه الأخطار.

نشــاط 4-3

تقيم المملكة العربية السعودية فعاليات عدة في مجال الأمن السيبراني، عدد مع معلّمك وزملائك بعضًا من الفعاليات التي أقيمت خلال السنوات الأخيرة.

اسم الفعالية	تاريخ الفعالية	الجهة المنظمة

- طبّــق مع الطلبــة طرائق الإبلاغ عــن الجرائم الســيبرانية، قــد يكون نشــاطًا داخــل الفصل الدراســي، أو نشــاطًا خارجيًّــا يحــاول الطالب الوصول إلى طريقة الإبلاغ المناسبة حسب نوع الجريمــة الســيبرانية، مع الإشــارة لهم إلى أن طريقة الإبلاغ تختلف من جهة إلى أخرى، وقد تختلف مــع الوقت طريقة الوصول إلى الموقع المطلوب بأســباب تحديثــات المواقع، وأن دور الطالــب هنــا يكمــن فــي محاولــة البحث عن الطريقة الجديدة إن اضطر لذلك.

طرائق الإبلاغ عن الجرائم السيبرانية بالمملكة العربية السعودية

نشــاط 5-3

اكتشــف طريقة الإبلاغ المناسبة عن الجريمة السيبرانية بمختلف أنواعها بمسح رمز الاستجابة السريع لكل جهة في الجدول الآتي:

الجهة الحكومية	رمز الاستجابة	طريقة الإبلاغ (موقع ويب، تطبيق هاتف، رقم اتصال، بريد إلكتروني، رسائل نصية)
الهيئة الوطنية للأمن السيبراني		.....
وزارة الداخلية		.....
الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر		.....
هيئة الاتصالات وتقنية المعلومات		.....

- يخصص لموضوع نظام مكافحة جرائم المعلوماتية حصة دراسية مستقلة لتوجيه تركيز الطلبة الكامل إليها؛ لما لها من أهمية في ممارساتهم اليومية.
- ابدأ بمناقشة الطلبة عن الهدف من وجود قانون مكافحة جرائم المعلوماتية، وناقشهم عن الآثار المترتبة إذا ازدادت المخالفات وعند عدم وجود نظام يردعها، ومدى ضررها على المستوى الفردي والاجتماعي والاقتصادي.
- أثناء استعراض مواد النظام ركّز على نقطتين رئيستين: (مدة عقوبة السجن، مقدار المخالفة المالية) لكل مادة من المواد المذكورة في الدرس.
- استعرض مواد نظام مكافحة جرائم المعلوماتية السعودي المذكورة، واجعل الطلبة يقرأون نص كل مادة مع التوقف عندها، وناقشهم عن المخالفة وعقوبتها لتساعد الطلبة بالتركيز على نوع المخالفة، وأنها تبدأ من الممارسات البسيطة وتتدرج إلى المخالفات الكبيرة مع ارتفاع العقوبات بشكل متوالي.
- بعد الانتهاء من استعراض جميع المواد التي تحمل المخالفات، وجه الطلبة بحل الأنشطة التي تتبع مواد نظام مكافحة جرائم المعلوماتية كما يأتي:
- نشاط (3-6): ينفذه الطالب بشكل فردي ليظهر مدى استيعابه للمخالفات، ومدى تمكّنه منها.
- نشاط (3-7): فتح المجال للطلاب بشكل جماعي لتذكّر أي ممارسات رقمية يمكن تصنيفها كمخالفات حسب النظام، وكتابة الواضح منها بعد اتفاق المجموعة عليها، وفيها دلالة على مدى استيعابهم لمواد النظام.
- نشاط (3-8): يقترح الطلبة بشكل جماعي الفوائد التي يمكن أن تعود على المجتمع والفرد السعودي من إقرار نظام مكافحة الجرائم المعلوماتية.

نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية

أقرت حكومة المملكة العربية السعودية نظام مكافحة جرائم المعلوماتية عبر جلسة مجلس الوزراء بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ. يتكون النظام من (16) مادة، ويتضمن النظام التعريف بالألفاظ والعبارات التي تخص النظام، والهدف من تطبيقه، وعقوبات مرتكبي جرائم المعلوماتية بالمملكة العربية السعودية. يهدف نظام مكافحة جرائم المعلوماتية -كما نصّ في النظام-إلى الحد من وقوع جرائم المعلوماتية، وتحديد الجرائم والعقوبات المقررة لكل منها، وذلك لتحقيق الأهداف الآتية:

173

1. المساعدة على تحقيق الأمن المعلوماتي.
2. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية، والشبكات المعلوماتية.
3. حماية المصلحة العامة، والأخلاق، والآداب العامة.
4. حماية الاقتصاد الوطني.

نشاط 6-3

بعد اطلاعك على مواد نظام مكافحة جرائم المعلوماتية، بيّن نوع العقوبات التي تتوافق مع مواد النظام للممارسات الرقمية الآتية:

م	الممارسة الرقمية	المادة المتوافق معها	مدة عقوبة السجن	مبلغ الغرامة المالية
1	الدخول إلى البيانات الائتمانية أو البنكية دون أي تصريح قانوني.			
2	تصوير شخص يمشي في أحد شوارع مدينتك.			
3	إنشاء مواقع غير قانونية.			
4	الاطلاع على البريد الإلكتروني لأحد زملائك في المدرسة.			
5	الترويج للمواقع والحسابات الإباحية.			
6	إلحاق الضرر بأحد أجهزة الحواسيب لإحدى الشركات التجارية.			
7	انتحال صفة شخص لإجراء عملية شراء إلكترونية			
8	التشهير بالآخرين في إحدى وسائل التواصل الاجتماعي.			
9	الدخول عنوة لإحدى أنظمة الدولة الرقمية والعبث بها.			
10	الدخول على شخصٍ ما وابتزازه لدفعه وإجباره على القيام بفعل معين.			

نشاط جماعي 7-3

تذكر مع مجموعتك خمس مخالفات معلوماتية وقعت في محيطك الشخصي، أو اطّلعت عليها عبر شبكة الإنترنت، وصنّفها وفق مواد نظام مكافحة جرائم المعلوماتية كما درستها.

م	المخالفة المعلوماتية	المادة المتوافق معها	مدة عقوبة السجن	مبلغ الغرامة المالية
1				
2				
3				

نشاط 8-3

من خلال المناقشة مع مجموعتك، بيّن الفوائد الإيجابية لإقرار وتطبيق نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية.

.....

.....

.....

.....

حل أنشطة وتدريبات الدرس

إثارة التفكير (1): هل يوجد فرق بين مرتكب الجريمة السيبرانية ومرتكب الإرهاب الإلكتروني من حيث النظام؟

نعم، فمرتكب الإرهاب يطبق عليه نظام مكافحة الإرهاب وهو مستقل عن نظام مكافحة الجرائم المعلوماتية.

حل نشاط (3-1): بالعودة لأركان الجريمة السيبرانية، استنبط دوافع ارتكاب الجرائم السيبرانية من قبل المجرمين السيبرانيين.

1. دوافع شخصية: تتمثل في الرغبة في التعلم لهذا المجال، ومحاولة التقدم والاستمرار والاكتشافات المتجددة.
2. دوافع مادية: تتمثل في الربح وكسب المال ومحاولة اتخاذ الجريمة السيبرانية مصدر دخل مغري بسبب كثرة العوائد المادية من العمليات المختلفة والطرق المتعددة.
3. دوافع المتعة: تتمثل في التحدي وإثبات الذات والشهرة على مستوى الشبكة بالإنجازات المتحققة.
4. الرغبة في الانتقام: تتمثل في الانتقام من شخص ما أو مؤسسة تعامل المجرم معها سابقًا، أو لاختلافات دينية، أو مالية، أو اجتماعية.
5. دوافع أخرى: تتمثل في التنافس بين الدول سياسيًا أو عسكريًا أو بين المنظمات التجارية والشركات الكبرى لتحقيق التقدم في المجال.

حل تدريب (3-1): بناء على اطلاعك على قائمة الأنشطة الإجرامية في جدول (3-1)، صنّف الممارسات الإجرامية عبر تحديد نوع النشاط الإجرامي لكل ممارسة في الجدول الآتي:

م	النشاط	رقم النشاط الإجرامي التابع له
1	إرسال ملف للآخرين لمعرفة ما لديهم من معلومات.	5
2	إنشاء موقع إلكتروني وهمي لبيع المستلزمات الطبية.	2
3	مطاردة شخص عبر شبكة الإنترنت ومضايقته وتهديده.	14
4	الدخول غير المصرح لموقع فندق وحجز غرفة.	2
5	فك حماية برنامج لغرض العمل عليه.	6
6	إنشاء صفحة تسجيل دورة تدريبية لاختبار القدرات لغرض سرقة الأموال.	2 – 12
7	إرسال رسالة احتيالية للبريد الإلكتروني من شركة شحن دولية.	2
8	التسلّل إلى إحدى خوادم شركات الاتصالات لحذف الفواتير المخزنة للمشتركين.	4
9	الحصول على ملف معلومات مهمة لمناقصة تجارية لإحدى الشركات.	4
10	إرسال ملف للآخرين لتشفير ملفاتهم وطلب مبلغ مقابل فك التشفير.	12-14
11	تعطيل نظام الإشارات المرورية.	10
12	إرسال صور غير أخلاقية عبر إحدى وسائل التواصل الاجتماعي.	11
13	تصوير الآخرين بكاميرا الجوال بدون علمهم.	14
14	استخدام البطاقة البنكية لصديقك من أجل الاشتراك بلعبة متصلة بالإنترنت.	14
15	إجراء توقيع مزيف لتوقيع مسؤول على إحدى الفواتير الإلكترونية.	1

حل تدريب (3-2): بيّن نوع الممارسات الرقمية من حيث انتمائها/عدم انتمائها لأنشطة الجرائم السيبرانية في الجدول الآتي:

م	الأفعال	انتماؤها للجريمة السيبرانية	
		ينتمي	لا ينتمي
1	الوصول إلى جهاز خادم (server) بدون تصريح من الجهة المالكة.	√	
2	إنشاء موقع إنترنت لتقديم خدمة تصميم خدمات إعلانية.		√
3	الشراء ببطاقة ائتمانية لشخص ما بدون إذنه.	√	
4	طلب بيانات شخصية من فرد عبر رسالة بالبريد الإلكتروني على شكل قالب تقديم وظيفة.		√
5	الوصول لبيانات تسجيل الدخول لإحدى وسائل التواصل الاجتماعي من طرف ثالث من غير المستخدم والشبكة الاجتماعية نفسها.		√
6	مساعدة الآخرين في مجال تعلّم البرمجة عبر مدونة خاصة.		√
7	إنشاء موقع إنترنت لتقديم معلومات مضللة تهدف إلى تغيير الحقائق.	√	
8	وضع ملف تنصت داخل جهاز خادم (server) للحصول على بيانات المشتركين.	√	
9	بيع السلع غير المشروعة عبر شبكة الإنترنت.	√	
10	التغريد عبر تطبيق تويتر عن أخبار غير صحيحة.	√	

حل نشاط (3-3): بناءً على ما ورد في القصة من أحداث، بيّن آثار الجريمة السيبرانية على الشركة عبر الإجابة عن الأسئلة الآتية: (إجابات مقترحة)

1. **ما دور الشركة المتوقع عندما أُعلمت عن مطالب المخترقين السابقة وقبل إتمام عملية الاختراق؟**
   - أخذ الموضوع بمحمل الجد، وعمل اجتماع بشأنه لمناقشة المطالبات، وتنفيذ الإجراءات بشأنها.
   - التبليغ عن المخترقين.
   - فحص نظام الحماية لأنظمة الشركة بشكل كامل وتحديثها.

2. **-هل ترى أن الأضرار التي تعرضت لها الشركة من جراء عملية الاختراق أضرت بسمعة الشركة؟ وضح ذلك.**

نعم، فعملية الاختراق تضر بسمعة الشركة، وكذلك تفقد سمعتها وثقتها عند العملاء، وتفقد مواكبتها للمنافسين في هذا المجال، وقد تقدر خسائرها المادية بمليارات الدولارات مما يضطرها إلى إعلان الإفلاس والإقفال.

3. **ناقش الأسباب التي ساعدت على إتمام عملية الاختراق.**
   1. نظام الحماية ضعيف جدًا مما سهّل الاختراق.
   2. عدم الاهتمام بإجراءات الأمن السيبراني، وتدريب الموظفين على ذلك.
   3. عدم استخدام أنظمة تشفير للبيانات والملفات.

4. **ما التصرف اللاأخلاقي الذي ورد في القصة؟ وبيّن سبب وقوع هذا التصرّف.**

تعاون أحد موظفي الشركة مع المخترقين، وقد يعود السبب إلى عدم وجود ولاء من الموظف للشركة، وعدم حصوله على الأمان والثقة من إدارة الشركة، بالإضافة إلى ضعف الوازع الديني لدى البعض.

5. **تحدث عن الفوائد التي تُستفاد من هذه القصة.**

1. **الاهتمام بإجراءات الحماية لأنظمة الشركة، وإنشاء إدارة للأمن السيبراني وحماية البيانات.**
2. **تحديث الأنظمة أمنيًا باستمرار ومتابعة الثغرات التي تكتشف بشكل مستمر من قبل المخترقين.**
3. **مراقبة الله سبحانه وتعالى في الممارسات الرقمية التي قد تؤدي إلى الإضرار بالآخرين معنويًا وماديًا.**
4. **تشفير البيانات المهمة في الأنظمة؛ لمنع وصول الآخرين إليها.**

حل نشاط (3-4): تقيم المملكة العربية السعودية فعاليات عدة في مجال الأمن السيبراني، عدد مع معلّمك وزملائك بعضًا من الفعاليات التي أقيمت خلال السنوات الأخيرة. (إجابات مقترحة)

اسم الفعالية	الجهة المنظمة في المملكة العربية السعودية
المنتدى الدولي للأمن السيبراني	الهيئة الوطنية للأمن السيبراني 2022
ATHACK ات هاك	الهيئة العامة للترفيه 2021
بلاك هات Black Hat	الهيئة العامة للترفيه 2022+ الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز

حل نشاط (3-5): اكتشف طريقة الإبلاغ المناسبة عن الجريمة السيبرانية بمختلف أنواعها بمسح رمز الاستجابة السريع لكل جهة في الجدول الآتي:

الجهة الحكومية	طريقة الإبلاغ (موقع ويب، تطبيق هاتف، رقم اتصال، بريد إلكتروني، رسائل نصية)
الهيئة الوطنية للأمن السيبراني	موقع ويب
وزارة الداخلية.	تطبيق كلنا أمن
الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر.	رقم اتصال، موقع ويب
هيئة الاتصالات وتقنية المعلومات	رسائل نصية، موقع ويب

حل نشاط (3-6): بعد اطلاعك على مواد نظام مكافحة جرائم المعلوماتية، بيّن نوع العقوبات التي تتوافق مع مواد النظام للممارسات الرقمية الآتية. (إجابات مقترحة)

م	الممارسة	المادة المتوافق معها	مدة عقوبة السجن	مبلغ الغرامة المالية بالريال
1	الدخول إلى البيانات الائتمانية أو البنكية دون أي تصريح قانوني.	الرابعة	ثلاث سنوات	مليونان
2	تصوير شخص يمشي في أحد شوارع مدينتك.	الثالثة	سنة واحدة	500 ألف
3	إنشاء مواقع غير قانونية.	السادسة	خمس سنوات	3 ملايين
4	الاطلاع على البريد الإلكتروني لأحد زملائك في المدرسة.	الثالثة	سنة واحدة	500 ألف
5	الترويج للمواقع والحسابات الإباحية.	السادسة	خمس سنوات	3 ملايين
6	إلحاق الضرر بأحد أجهزة الحواسيب لإحدى الشركات التجارية.	الخامسة	أربع سنوات	3 ملايين
7	انتحال صفة شخص لإجراء عملية شراء إلكترونية.	الرابعة	ثلاث سنوات	مليونان

حل نشاط (3-8): (إجابات مقترحة)

لحفظ النظام وردع المخالفات، وحماية الخصوصية عبر الإنترنت وفي الأماكن العامة.

سُلَّم تقدير مشروع الدرس:

يستخدم سُلَّم التقدير لتقييم مشاريع الطلبة بنهاية كل درس، وتجمع نقاط كل مؤشر للحصول على التقييم النهائي للطالب أو المجموعة المنفذة للمشروع، ومن المهم أن يُعرض السُلَّم على الطلبة قبل بدء العمل على المشروع بوقت كافٍ حتى يتسنى لهم تنفيذ المشروع بناءً على المعايير والمؤشرات في سُلَّم التقدير.

معايير التقييم	مؤشرات الأداء	ممتاز (5)	جيد جدًا (4)	جيد (3)	مقبول (2)	ضعيف (1)
جودة وتنظيم المعلومات	المعلومات المعروضة مرتبطة بالموضوع الرئيس	المعلومات مرتبطة بالموضوع، توجد بيانات وأمثلة، واحصائيات كافية تدعم الموضوع.	المعلومات مرتبطة بالموضوع، توجد بيانات وأمثلة، واحصائيات مناسبة تدعم الموضوع.	المعلومات مرتبطة إلى حد ما بالموضوع، توجد بيانات وأمثلة، واحصائيات قليلة تدعم الموضوع.	المعلومات مرتبطة إلى حد ما بالموضوع، لا توجد بيانات وأمثلة، واحصائيات تدعم الموضوع.	المعلومات غير مرتبطة بالموضوع، لا يوجد أمثلة واحصائيات وبيانات تدعم الموضوع.
	صحة وتنظيم المعلومات في العرض	المعلومات منظمة جدًا، الفقرات مصاغة بشكل ممتاز، والأفكار متسلسلة، واستخدام العناوين الفرعية صحيح، المعلومات حقيقية.	المعلومات أقل تنظيمًا، الفقرات مصاغة بشكل جيد، والأفكار متسلسلة، واستخدام العناوين الفرعية صحيح، المعلومات حقيقية.	المعلومات شبه منظمة، الفقرات مصاغة بشكل مقبول، والأفكار شبه متسلسلة، واستخدام العناوين الفرعية شبه صحيح، المعلومات شبه حقيقية.	المعلومات شبه منظمة، الفقرات مصاغة بشكل ضعيف، والأفكار غير متسلسلة، واستخدام العناوين الفرعية شبه صحيح، المعلومات شبه حقيقية.	المعلومات غير منظمة، الفقرات ليست مصاغة بشكل سليم، وغير متسلسلة الأفكار، ولا العناوين الفرعية، والمعلومات غير حقيقية.
	الأخطاء الإملائية والنحوية والترقيم	لا يوجد أخطاء إملائية أو نحوية أو ترقيم.	أخطاء متوسطة إما إملائية أو نحوية أو ترقيم.	أخطاء إملائية أو نحوية قليلة.	أخطاء إملائية ونحوية أو ترقيم قليلة.	يوجد أخطاء كثيرة إملائية ونحوية وترقيم.
تسليم العمل	تسليم العمل للمعلم حسب الوقت	في الوقت المحدد.	تأخير أكثر من (يومين)	تأخير أكثر من (أربعة أيام)	تأخير أكثر من (ستة أيام)	تأخير أسبوع فأكثر.
مصادر المعلومات	التعدد في مصادر المعلومات	خمسة مصادر فأكثر.	أربعة مصادر.	ثلاثة مصادر.	مصدران اثنان.	مصدر واحد.
	التنوع في المصادر	قواعد البيانات، الموسوعات، محركات البحث، مواقع الهيئات والمنظمات.	قواعد البيانات، محركات البحث، مواقع الهيئات والمنظمات.	الموسوعات، محركات البحث.	محركات البحث، مواقع الهيئات والمنظمات.	محركات البحث فقط.
	توثيق المعلومات في العرض	التزام كلي بنظام التوثيق، استخدام (5) مراجع فأعلى.	التزام كبير بنظام التوثيق، استخدام (4) مراجع.	التزام متوسط بنظام التوثيق، استخدام (3) مراجع.	التزام ضعيف بنظام لتوثيق، استخدام (3) مراجع.	نظام التوثيق غير دقيق، استخدم أقل من (3) مراجع.
مواصفات العمل المطلوب	عدد الشرائح المطلوبة (بما فيها شريحتي العنوان والمراجع)	أكثر من 7 شرائح.	7 شرائح.	6 شرائح.	5 شرائح.	4 شرائح فأقل.
	الإخراج والتنسيقات (الخلفية، الألوان، نوع الخط، تنسيق المادة العلمية، حجم الخط) في العرض	تنسيق جذاب، حجم الخطوط متساوي، ونوع خط موحد، حجم عناوين بارز.	تنسيق جذاب إلى حد ما، حجم الخطوط متساوي، ونوع خط موحد، حجم عناوين واضح.	تنسيق متوسط الجاذبية، حجم الخطوط شبه متساوي، ونوع خط شبه موحد، حجم عناوين عادي.	تنسيق قليل الجاذبية، حجم الخطوط شبه متساوي، ونوع الخط شبه موحد، حجم عناوين عادي.	تنسيق غير جذاب، حجم الخطوط مختلف، ونوع الخط متنوع، حجم عناوين غير بارز.
	الإضافات في العرض	مجموعة من الرسومات والصور والجداول والزخارف.	مجموعة من الرسومات والصور والجداول.	مجموعة من الصور والجداول.	مجموعة من الصور، والرسومات.	لا يحتوي على إضافات.