

تم تحميل وعرض المادة من

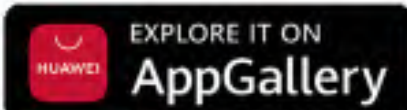
منهجي

mnhaji.com



موقع منهجي منصة تعليمية توفر كل ما يحتاجه المعلم
والطالب من حلول الكتب الدراسية وشرح للدروس
بأسلوب مبسط لكافة المراحل التعليمية وتوازيح
المناهج وتحاضير وملخصات ونماذج اختبارات وأوراق
عمل جاهزة للطباعة والتحميل بشكل مجاني

حمل تطبيق منهجي ليصلك كل جديد



قررت وزارة التعليم تدريس
هذا الكتاب وطبعه على نفقتها



المملكة العربية السعودية

وزارة التعليم
Ministry of Education

المواطنة الرقمية

التعليم الثانوي - نظام المسارات

السنة الثالثة

قام بالتأليف والمراجعة

فريق من المتخصصين



وزارة التعليم
يُوزع مجاناً للإسراع
Ministry of Education
2023 - 1445

طبعة 1445 - 2023

ح) وزارة التعليم ، ١٤٤٤ هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر
وزارة التعليم

المواطنة الرقمية - التعليم الثانوي - نظام المسارات - السنة
الثالثة. / وزارة التعليم. - الرياض ، ١٤٤٤ هـ.
٢٣٩ ص ؛ ٢٧×٢١ سم

ردمك : ٠ - ٤٥٣ - ٥١١ - ٦٠٣ - ٩٧٨

١ - المواطنة - تعليم - السعودية ٢ - الوعي الاجتماعي ٣ - التعليم
الثانوي - السعودية - كتب دراسية أ. العنوان
ديوي ٣٢٣, ٦٥ ١٤٤٤ / ٩٤٦٦

رقم الإيداع : ٩٤٦٦ / ١٤٤٤

ردمك : ٠ - ٤٥٣ - ٥١١ - ٦٠٣ - ٩٧٨

حقوق الطبع والنشر محفوظة لوزارة التعليم

www.moe.gov.sa

مواد إثرائية وداعمة على "منصة عين الإثرائية"



ien.edu.sa

أعزاءنا المعلمين والمعلمات، والطلاب والطالبات، وأولياء الأمور، وكل مهتم بالتربية والتعليم:
يسعدنا تواصلكم؛ لتطوير الكتاب المدرسي، ومقترحاتكم محل اهتمامنا.



fb.ien.edu.sa

أخي المعلم/أختي المعلمة، أخي المشرف التربوي/أختي المشرفة التربوية:
نقدر لك مشاركتك التي ستسهم في تطوير الكتب المدرسية الجديدة، وسيكون لها الأثر الملموس في دعم
العملية التعليمية، وتجويد ما يقدم لأبنائنا وبناتنا الطلبة.



fb.ien.edu.sa/BE



وزارة التعليم

Ministry of Education

2023 - 1445

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



وزارة التعليم

Ministry of Education

2023 - 1445

المقدمة

نعيش اليوم في عالم متسارع التغير، ومتسع الآفاق، أحاطت به التقنيات الرقمية من جميع النواحي، مما يدعونا لضرورة مواكبته ليس معرفياً وتقنياً فحسب؛ بل أيضاً فكرياً، وأخلاقياً، واجتماعياً، وصحياً، وأمنياً، وهذا ما قاد وزارة التعليم لأخذ زمام المبادرة في ترسيخ مبادئ المواطنة الرقمية لدى الناشئة. وقد أعد فريق من الخبراء التربويين مقرر المواطنة الرقمية بالمرحلة الثانوية بما يتلاءم ويتسق مع المعايير العالمية للمواطنة الرقمية، آخذين بالاعتبار أحدث المستجدات التقنية، والتطورات العالمية، والتوجهات التربوية الحديثة، والقيم الإسلامية، ورؤية المملكة العربية السعودية 2030 التي تسعى لتعزيز القيم الإسلامية والهوية الوطنية، بما يمكن الطلبة الاندماج في البيئة الرقمية بمسؤولية وثقة للتطور كفداة يتركون أثراً ذي مغزى في حياة الآخرين .

يسعى هذا المقرر من خلال وحداته الثلاث إلى تزويد طلبتنا بالكفايات التي يحتاجون إليها؛ ليصبحوا مواطنين مسؤولين في العالم الرقمي، حيث تهدف الوحدة الأولى (الوعي والثقافة الرقمية) إلى التعريف بمفهوم المواطنة الرقمية، وفهم تأثيرات التقنية، والكفايات الرقمية وكيفية تطويرها ذاتياً باستخدام التقنيات. كما يهدف إلى تعريف الطالب بالتغيرات التي أحدثتها التقنيات الرقمية في عدة مجالات كالتجارة الإلكترونية، والإعلام الرقمي، والخدمات الرقمية.

بينما تهدف الوحدة الثانية (الاحترام والمسؤولية الرقمية) إلى تمكين المواطن الرقمي من إدارة حضوره الرقمي بوعي ومسؤولية بما يعكس هويته الإسلامية والوطنية، وتزويده بالمعارف، والمهارات، والقيم التي تساعد على بناء بصمة وسمعة رقمية إيجابية، والوعي بأنواع العلاقات الرقمية، وكيفية إدارتها بشكل فعال، إضافة إلى الانتباه لأشكال العنف الرقمي، وكيفية التعامل معها، والتمكّن منها للوصول إلى حالة الاتزان الرقمي.

أما الوحدة الثالثة (الأمان والحماية الرقمية) فتهدف إلى التوعية بالإجراءات التي تجعل المواطن الرقمي واعياً لممارساته الرقمية، وتمكّناً بوسائل الحماية من الأخطار والتهديدات الرقمية التي يواجهها في العالم الرقمي، ومعرفة القوانين والأنظمة التي تنظم التعامل بين الأفراد مع بعضهم البعض، وبين الأفراد والجهات الحكومية والخاصة، وكيف يسهم المواطن الرقمي في توعية الآخرين للعيش في عالم آمن.



أخي الطالب ...

خلال رحلة مقرر المواطنة الرقمية ستتوقف في ثلاث محطات رئيسة تهدف إلى تزويدك بالمعارف، والاتجاهات، والمهارات، التي تجعلك قادرًا على تمييز آثار العالم الرقمي على حياتك وتعاملاتك، وتكون قادرًا على التعامل معه بمسؤولية واحترام، وقادرًا على حماية نفسك فيه؛ لتصبح مواطنًا رقميًا واعيًا.

|| خارطة الكتاب



وستشاهد أثناء رحلتك في هذا المقرر بعض الرموز، وفيما يأتي دلالاتها:

الرموز	دلالاتها
	إثارة التفكير
	إضاءة
	إثراء
	قصة
	غذاء للفكر
	نقاط مهمة
	النشاط (فردى، جماعى)، مجتمعى
	التدريب (فردى، جماعى)
	بطاقة المواطن الرقمى
	مشروع الدرس

العناوين	دلالاتها
أقيّم ما تعلّمت فى الوحدة	عبارة عن سلم متدرج يمكن الطالب من قياس درجة تمكنه من مخرجات التعلم للدرس.
خارطة مفاهيم الوحدة	خريطة مفاهيمية تعرض المواضيع التى غُطِّيت فى الوحدة بشكل رسمى.
تقويم الوحدة	أسئلة تُقدّم فى نهاية كل وحدة تساعد على تقييم اكتسابك للمعارف الواردة خلال الوحدة.
دليل مصطلحات الكتاب	دليل لعرض جميع المصطلحات الواردة فى الكتاب وتعريفاتها.



فهرس المحتويات

الصفحة	الدرس
الوحدة الأولى: الوعي والثقافة الرقمية	
10	مقدمة الوحدة الأولى
12	مقدمة في المواطنة الرقمية
22	آثار العالم الرقمي
34	الخدمات الرقمية
42	الوعي الإعلامي الرقمي
56	الوعي بالتعامل مع التجارة الإلكترونية
72	تقويم الوحدة الأولى
الوحدة الثانية: الاحترام والمسؤولية الرقمية	
78	مقدمة الوحدة الثانية
80	الهوية الرقمية
96	التواصل والعلاقات الرقمية
118	العنف الإلكتروني
138	الصحة والالتزان في العالم الرقمي
154	تقويم الوحدة الثانية



الوحدة الثالثة: الأمان والحماية الرقمية	
160	مقدمة الوحدة الثالثة
162	الجرائم السيبرانية، وجهود مكافحتها محلياً ودولياً
180	الحماية من التهديدات الرقمية
196	الخصوصية وحماية البيانات
216	حماية الملكية الفكرية للمحتوى الرقمي
234	تقويم الوحدة الثالثة
239	دليل مصطلحات الكتاب.





الوحدة الأولى



وزارة التعليم

Ministry of Education

2023 - 1445

الوعي والثقافة الرقمية

Digital Culture and Awareness

تسلط الوحدة الضوء على القسم الأول لمقرر المواطنة الرقمية الذي يشمل على الوعي والثقافة الرقمية، حيث يقدم للمتعلّم بدايةً عن مفهوم المواطنة الرقمية، وكيف يتّسم المواطن بالمواطنة الرقمية، ومدى تأثيرها على العالم الواقعي، وما أحدثته من تغيّرات في الحياة، والخدمات، والأعمال، وكيف أثر العالم الرقمي في تحوّل الخدمات الحكومية إلى خدمات رقمية لمواكبة التحول الرقمي المستمر، كما تكمل الوحدة دورها بتهيئة الطالب ليكون متعلّمًا دائمًا، ومستمرًا مدى الحياة، وواعيًا لممارساته الرقمية أثناء التعامل مع الإعلام الرقمي المتجدد، وإعطاءه مجموعة من النصائح في مجال التعامل مع التجارة الإلكترونية.

متطلبات الوحدة

تحتوي بعض الدروس على تطبيقات عملية تحتاج إلى توفير جهاز حاسوب، خدمة إنترنت، برمجيات نظام التشغيل ويندوز، تطبيقات الهواتف الذكية.



أهداف التعلم

بنهاية هذه الوحدة سيكون الطالب قادراً على:

1. تعلم أساسيات المواطنة الرقمية، ومحاورها.
2. إيضاح علاقة المواطنة الرقمية بالهوية الإسلامية، وأدوار المواطن الرقمي في العالم الرقمي.
3. بيان أهمية تأثير العالم الرقمي في تغير العالم الواقعي وتأثيره على كل من الثقافات، والتعليم، والمهن المستقبلية، وتنمية المجتمعات.
4. دور التحول الرقمي في توفير منصات التدريب الرقمية المختلفة لتطوير المهارات.
5. الاطلاع على الخدمات الرقمية الحكومية واستخدامها بمهارة.
6. تبيين دور الخدمات الرقمية الحكومية في رفع مستوى رفاهية المواطن والمقيم.
7. تطبيق خطوات مهارة القراءة الجانبية للتحقق من صحة المادة الإعلامية الرقمية.
8. إنتاج مادة إعلامية يلتزم فيها الطالب بقوانين نظام المطبوعات والنشر في المملكة العربية السعودية.
9. مناقشة مفهوم الإعلام الرقمي، وخصائصه، وأهم وسائله.
10. استيعاب مفهوم التجارة الإلكترونية، وخطوات الشراء الآمن من المتاجر الإلكترونية.
11. استشعار أهمية التجارة الإلكترونية في تحسين جودة الحياة، وجهود المملكة العربية السعودية في توفير ذلك.





مقدمة في المواطنة الرقمية

الدرس الأول

مخرجات التعلم:

- أعرف مفهوم المواطنة الرقمية.
- أشرح أهمية تعلم المواطنة الرقمية.
- أحدد محاور المواطنة الرقمية.
- أوضح علاقة المواطنة الرقمية بالهوية الإسلامية، ودور الأمة الإسلامية تجاه المحافظة على هويتها وثقافتها.
- أبين أدوار ومسؤولياتي تجاه الأجيال الرقمية.



مصطلحات الدرس:

- المواطنة الرقمية (Digital Citizenship).
- المهاجرون الرقميون (Digital Immigrants).
- المواطنون الرقميون (Digital Citizens).

التهيئة

نشاط



1-1

اربط العبارات في الجدول الآتي مع الصور المناسبة لها، في حالة الربط بشكل صحيح لأكثر من نصف عدد الصور فهي دلالة على وجود خلفية معرفية لديك عن مفهوم المواطنة الرقمية.

1. علامة توضع قبل موضوع النقاش تساعد في زيادة التفاعل بين مستخدمي وسائل التواصل الاجتماعي.	2. أثر المعلومات الذي تتركه وراءك على موقع الويب.	3. الاستخدام المفرط للتقنية الرقمية.
4. الاستفادة من التقنية الرقمية في تحسين الصحة الجسدية والنفسية.	5. الإساءة للأشخاص وإهانتهم عبر الإنترنت.	6. ضرر يمكن أن يصيب جهاز الحاسوب الخاص بك.
7. إنستغرام، سناب شات، تيك توك، Snapchat، تويتر، تسمى ...	8. بريد إلكتروني غير مرغوب فيه.	9. فهم ما يشعر به شخص آخر.
10. التحديث لحماية معلوماتك الخاصة.	11. تستخدم للتعبير عن المشاعر أثناء المحادثات النصية.	12. طريقة تساعد في التقليل من الوقت الذي يقضيه الشخص على جهازه.
13. نسخ عمل الآخرين وادعاء أنه ملكك.	14. الوعي الإعلامي الرقمي يساعد في تمييز الأخبار الحقيقية من الزائفة.	15. يجب أن تجعلها معقدة وتحفظ بها لنفسك.

	الانتقال الرقمي		إعدادات الخصوصية		أخبار مزيفة
	التمتع الإلكتروني		الإدمان الرقمي		البصمة الرقمية
	وقت الشاشة		كلمة المرور		الفيروسات
	وسم		التعاطف		وسائل التواصل الاجتماعي
	رموز تعبيرية		البريد العشوائي		الصحة الرقمية

|| مفهوم المواطنة الرقمية (Digital Citizenship)



يزيد عدد المتصلين بالإنترنت في العالم على (4) مليار شخص، وهو رقم يمثل أكثر من نصف سكان العالم البالغ (8) مليار نسمة ويزداد هذا العدد بشكل مستمر، ويستخدم هؤلاء الأشخاص الإنترنت لأغراض متعددة كالعمل والتعليم والترفيه والصحة والتجارة وغيرها مشكلين بذلك مجتمعاً عالمياً رقمياً مترابطاً رغم اختلاف مواقع المستخدمين وهوياتهم ولغاتهم، وتؤثر سلوكيات كل منهم بشكل كبير على الآخرين في هذا الفضاء الواسع.

كما هو الحال في أي مجتمع يتصرف المواطنون وفق أعراف ومعايير وقوانين البلد التي يقطنونها، لدى العالم الرقمي أعرافاً وقوانين وسلوكيات يجب على من يتصل به الالتزام بها، وعلى الرغم من أن معظم سكان عالم اليوم من المواطنين الرقميين اندمجوا اندماجاً تاماً في استخدام التقنيات، يبقى السؤال المهم هنا هو هل يستخدمونها بشكل ملائم؟ وهل هم على وعي بأدوارهم ومسؤولياتهم تجاه المجتمع العالمي الرقمي؟

إن الوعي بهذه الأدوار والمسؤوليات هو ما يبني مفهوم المواطنة الرقمية التي تسهم في بناء بيئة آمنة لمواطنيها الرقميين، فماذا تعني المواطنة الرقمية؟

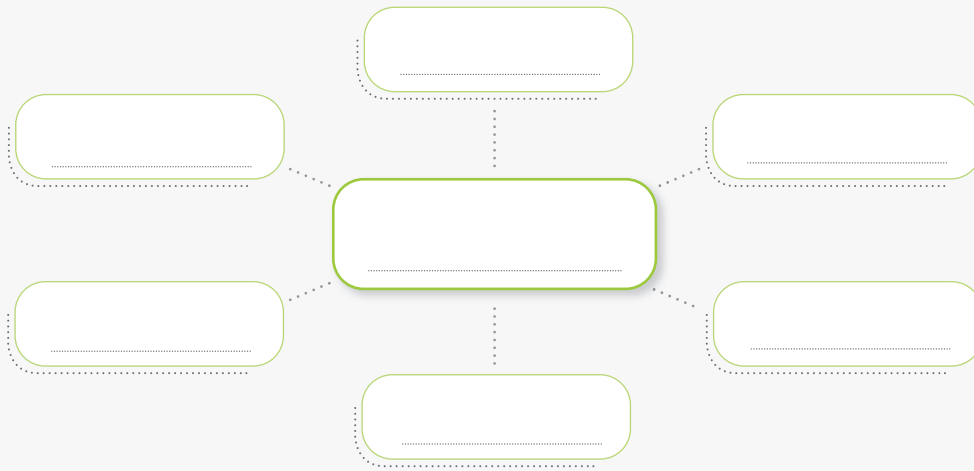
تصف المواطنة الرقمية العلاقة التي تربط الأشخاص بالعالم الرقمي، وتهدف إلى توفير البيئة الملائمة والإيجابية للأفراد بالتعامل والعيش في العالم الرقمي بصحة وأمان وتفاعل يضمن لهم حقوقهم، ويلزمهم بواجباتهم ومسؤولياتهم داخل هذا العالم المفتوح أمام الجميع. يوجد العديد من التعاريف للمواطنة الرقمية، منها:

- مجموعة القواعد والضوابط والمعايير والمبادئ التي تضمن الاستخدام الأمثل والأمن والوعي للتقنية.
- إعداد الفرد لمجتمع مليء بالتقنيات الرقمية.
- الالتزام بقواعد السلوك المناسب والمسؤول فيما يتعلق باستخدام التقنيات الرقمية.

نشاط



حلل التعاريف السابقة، واستنتج العناصر الأساسية التي تبنى عليها المواطنة الرقمية.



اقترح تعريفاً من إنشاءك للمواطنة الرقمية.

أهمية تعلم المواطنة الرقمية

مع تزايد أعداد مستخدمي الإنترنت من فئة الشباب والشابات في المملكة العربية السعودية، تزداد أهمية تنمية المواطنة الرقمية لديهم أثناء مراحلهم الدراسية حتى تنشأ مواطنتهم الرقمية مع مواطنتهم المحلية والعالمية جنباً إلى جنب، حيث يتوافق مع ما نصّ عليه برنامج التحول الرقمي 2020م ضمن رؤية المملكة العربية السعودية 2030م في تعزيز القيم والمهارات لدى الطلاب، وبناء شخصيتهم الإسلامية والفكرية. تكمن أهمية تعلم الطلاب للمواطنة الرقمية في تحقيق مجموعة من الأهداف كما في شكل (1-1).

- استخدام معارفهم ومهاراتهم وقيمهم من أجل حماية وتعزيز حقوقهم في العالم الرقمي كالحرية والخصوصية والأمن.
- إرشادهم لكيفية استخدام خدمة الإنترنت، والتقنيات الرقمية بمسؤولية وأمان، والمشاركة باحترام.
- العثور على المصادر الموثوقة عبر شبكة الإنترنت، وتجنب انتهاك حقوق المستخدمين.
- زيادة وعي الطلاب بالجوانب الإيجابية والسلبية في العالم الرقمي كالتعرض للاحتيال وللمعلومات المضللة التي قد يواجهونها أو يتعرضون لها بشكل يومي.
- زيادة الوعي عن المخاطر الصحية جراء عدم التوازن في استخدام التقنية الرقمية.
- إكسابهم مهارات في السلوك الإيجابي الرقمي كتحمل المسؤولية الشخصية، والإنتاجية والتعاون والتفاعل الإيجابي مع الآخرين، والشراء والبيع عبر شبكة الإنترنت.

أهمية تعلم المواطنة الرقمية



شكل (1-1): أهمية تعليم المواطنة الرقمية للطلاب

|| محاور المواطنة الرقمية

تتنوع موضوعات المواطنة الرقمية لتغطي كل ما يتعلق بوجود الأفراد الواعي والمسؤول والأمن على شبكة الإنترنت، ويمكن تصنيف موضوعات المواطنة الرقمية لثلاثة محاور رئيسة (شكل 2-1):



شكل (2-1): محاور المواطنة الرقمية

|| المواطنة الرقمية وهويتي الإسلامية

حرص الدين الإسلامي الحنيف من خلال تعاليمه وتشريعاته على بناء شخصية المسلم التي تمكنه من حمل أمانة هذا الدين ، لذلك حرص الإسلام في كثير من تشريعاته على تحقيق الاستقلال والمسؤولية في شخصية المسلم، إذ يرشدنا الدين الإسلامي إلى أن كل إنسان مسؤول عن أعماله، وأنه سيحاسب على ما اقترفته يده ، وجنته جوارحه، قال تعالى: ﴿كُلُّ نَفْسٍ بِمَا كَسَبَتْ رَهِينَةٌ﴾ [المدثر: 38]، وقال تعالى: ﴿إِنْ كُلُّ مَنْ فِي السَّمَوَاتِ وَالْأَرْضِ إِلَّا آتَى الرَّحْمَنِ عَبْدًا﴾ [١٣] لَقَدْ أَحْصَاهُمْ وَعَدَّهُمْ عَدًّا ﴿١٤﴾ وَكُلُّهُمْ عِندَهُ يَوْمَ الْقِيَمَةِ فَرْدًا ﴿١٥﴾ [مريم : 93-95].



يتوافق مفهوم المواطنة الرقمية مع تشريعات الإسلام، فالتواجد المسؤول والأخلاقي والأمن عبر استخدام التقنيات يحاسب عليه الفرد كما في العالم الواقعي. فكل منا مسؤول عن استخدامه للإنترنت ومحاسب عليه إن كان خيراً فخير وإن كان شراً فشر، وكل فرد مؤتمن على دينه لعكس هويته الإسلامية من خلال استخدامه وبحثه وإضافاته ومساهماته قال تعالى: ﴿إِنَّ السَّمْعَ وَالْبَصَرَ وَالْفُؤَادَ كُلُّ أُولَئِكَ كَانَ عَنْهُ مَسْئُولًا﴾ [الإسراء: 36]، وكذلك عبر تعاملاته مع الآخرين واحترام حقوقهم ومشاعرهم وممتلكاتهم الرقمية. وكل منا مؤتمن على نفسه، فيجب أن يكون واعياً بدرجة كافية بالأخطار التي قد تواجهه في العالم الرقمي، والحرص على الاهتمام بتطبيق إجراءات الأمن، واتباع قواعد السلامة. يكمن الدور المناط بالمواطن الرقمي تجاه الحفاظ على الهوية والثقافة الإسلامية في محاولة ما يأتي (الشكل 3-1):

رسم طريقه في التعامل مع التقنية الرقمية، والاستفادة منها، وعدم الانعزال عنها، وأن يكون المواطن الرقمي المسلم مشارك فعال ومؤثر إيجابي، بما يضمن الحفاظ على الثقافة والهوية الإسلامية.

نشر الثقافة الإسلامية وإبراز صورتها لدى مختلف الثقافات بما تحمله من الحرية والعدالة والمساواة والتسامح والإخاء وغيرها من المبادئ والقيم عبر إنتاج ونشر المحتوى الرقمي.

التعرف على الثقافات الأخرى بالاستفادة منها بما يزيد الرصيد الثقافي الإسلامي، والتعاون والاشتراك معهم في الأحداث والفعاليات الثقافية بما يحقق الانتماء الدولي.

شكل (3-1): دور المواطن الرقمي في المحافظة على الهوية والثقافة الإسلامية



بعد قراءتك للنص أعلاه، ومن خلال دورك كمواطن رقمي واعي اذكر عددًا من الأمثلة والممارسات العملية الواقعية من الأنظمة أو التطبيقات أو الخدمات التي دلت على حفاظنا على ثقافتنا وهويتنا الإسلامية، وإظهار قيمنا ومبادئنا في العالم الرقمي.

1. إنشاء تطبيقات المصحف الشريف.

2.

3.

4.

5.

6.

الأجيال الرقمية



أسهم التطور التقني عبر العصور في تغيير حياة الإنسان، ولا تؤدي التقنية دورًا في تغيير وتحسين وتطوير حياة الانسان فحسب بل في تغيير العديد من الصفات التي يتصف بها أفراد الجيل في كل عصر حتى باتت ملامح كل جيل مختلفة عن الجيل الآخر، وكان لفترة ولادة المنتمين للجيل الرقمي وتوفر التقنيات دور أساسي في تحديد الأجيال الرقمية، وبناء على هذين العاملين تم تقسيم الأجيال إلى قسمين أساسيين:

1. جيل ما قبل التقنية: وينقسم هذا الجيل إلى قسمين: القسم الأول يرفض التعامل مع التقنية، بينما القسم الآخر سعى للتعامل معها، ولذا أطلق عليهم مسمى المهاجرون الرقميون (Digital Immigrants).

2. الجيل المعاصر للتقنية: وهم من وُلد أثناء وجود التقنية ويطلق عليهم مسمى المواطنون الرقميون (Digital Citizens) وينقسمون لعددٍ من الأجيال بناءً على فترة ولادتهم، ونوع التقنيات الرقمية التي تزامنت مع جيلهم.



وفقاً لتنظيم الأجيال والتطور الهائل في التقنية سيكون هناك جيل جديد يكون العالم الرقمي والواقع الافتراضي مكاناً لحياته، بل سيندمج مع الواقع الافتراضي بشكل أكبر من الواقع الحقيقي، وقد أقدمت العديد من الشركات والمنظمات لتحويل خدماتها للتعامل مع الواقع الافتراضي استجابة لخصائص هذا الجيل الذي يعتمد على عالم الميتافيرس (Metaverse) وهو العالم الذي يندمج في العالم الافتراضي باستخدام تقنيات مثل: الواقع الافتراضي (Virtual Reality)، والواقع المعزز (Augmented Reality)، والواقع الممتد (Extended Reality).



إضاءة

نشاط فردي



5-1

ما خصائص الجيل الرقمي؟



- هل يوجد اختلاف في تعامل الفرد في العالم الواقعي عنه في العالم الرقمي؟
- كيف كانت الحياة قبل تطور التقنية الرقمية؟ وكيف كان الناس يتعاملون ويتواصلون؟ وكيف يمكن أن تكون حياتك بدون التقنية الرقمية؟

- تذكر قول رسول الله ﷺ (اتَّقِ اللَّهَ حَيْثُمَا كُنْتَ وَأَتِّعِ السَّيِّئَةَ الْحَسَنَةَ تَمْحُهَا، وَخَالِقِ النَّاسَ بِخُلُقٍ حَسَنٍ) [أخرجه الترمذي : 1987]
- المواطنة الرقمية تشمل المعارف والقيم والاتجاهات والمهارات، وأن اكتساب المعارف دون امتلاك مهارة لتطبيقها لا يجعلك مواطناً رقمياً واعياً.



مشروع الدرس



مع اختلاف الأجيال بين كل من الآباء والأبناء، تحدّث إلى والديك أو أحد معلّميك أو أحد أقاربك الأكبر سنّاً، ووجه لهم الأسئلة الآتية:

- ما واقع حياتهم قبل التقنية الرقمية؟
- كيف دخلت التقنية إلى حياتهم؟
- كيف غيرت التقنية الرقمية حياتهم؟
- ما إيجابيات وسلبيات التقنية الرقمية من وجهة نظرهم؟
- ثم أعد تقريراً يلخّص حوارك معهم، مع توضيح وجهة نظرك في كيف اختلف استخدام الجيل الحالي عن السابق في استخدام التقنية الرقمية؟
- كيف تستطيع التكامل مع والديك الذين قد يكونون مختلفين معك في الجيل الرقمي؟





آثار العالم الرقمي

الدرس الثاني



مخرجات التعلم:

- أذكر أمثلة على تأثير العالم الرقمي في تطور وتغير الثقافات.
- أناقش كيف أسهم العالم الرقمي في تعزيز التعليم وتطويره.
- أكتشف دور التحول الرقمي في تغيير مهن المستقبل.
- أستخدم إحدى منصات التدريب الرقمية لتطوير كفاياتي المهنية.
- أناقش دور الذكاء الاصطناعي والبيانات الضخمة في تنمية المجتمعات.

مصطلحات الدرس:

- العالم الرقمي (Digital World).
- الذكاء الاصطناعي (Artificial Intelligence).
- البيانات الضخمة (Big Data).

التهيئة

يناقش الابن وليد والده المتخصص في التقنية حول أجهزة المنزل الحديثة التي تم شراؤها، وسعي والده لاقتناء كل جديد من الأجهزة الذكية الحديثة لتحل محل الأجهزة القديمة في المنزل، وذلك لقلب المنزل من منزل اعتيادي إلى منزل ذكي، بما في ذلك تحويل جميع أجهزة المنزل الكهربائية والميكانيكية والإلكترونية إلى أجهزة ذكية يتم التحكم بها بشكل تلقائي، وعن بعد بواسطة شبكة الإنترنت، ويتساءل وليد:

- هل ستحل الآلة مكان الإنسان؟
- هل نحن على استعداد لدخول نظام مهني جديد في مجال العمل؟
- هل يمكن أن يغير العالم الرقمي طرائق تواصلنا الاجتماعية مع بعضنا البعض؟
- هل يمكن أن نثق بالتقنية الرقمية وما تقدمه لنا في جميع مجالات حياتنا؟

تأثير العالم الرقمي في تطور وتغير الثقافات

إن تأثير التقنية الرقمية على الثقافة والتقاليد والقيم الاجتماعية من التحديات في العالم الرقمي (Digital World)، ويمكن معرفة مدى التأثير وفقاً لكيفية تأثيرها على المجتمعات، وعلى الأنشطة البشرية. فثقافة المجتمع هي انعكاس لمعتقداته، وتقاليد وممارساته، تُعد اللغة والتعليم والتنقل والصناعة والفن والدين أجزاء حيوية من الحضارة المتأثرة بالتقنية الرقمية، ولذا فإن التقنية الرقمية يجب أن تكون متواكبة مع الظروف الثقافية والاجتماعية التي لا يكون هبات

تضارباً بين التقدم التقني والحفاظ على القيم الثقافية.



تعد صناعة المعلومات في القرن الحالي من أبرز الثروات التي تقارن بها الشعوب كالغذاء والدواء والنفط، ويمكن تحديد تصنيف دولة من بين الدول حسب مستوى ثقافتها المعلوماتية، ومدى ما توصلت له في مجال الاستفادة من /أو الصناعة في مجال التقنية الرقمية، لذا فهي سبب رئيس للتقدم في العلوم الطبية، والهندسية، والاقتصادية، والصناعية، وغيرها من المجالات.

نشاط



للعالم الرقمي تأثير واضح على ثقافات المجتمعات والأفراد في عاداتهم وتقاليدهم وممارساتهم، اذكر على هيئة نقاط في الجدول أدناه أمثلة على إسهام العالم الرقمي في تغيير عادات وممارسات الأفراد والمجتمعات قبل دخول التقنية الرقمية إليها وبعد دخولها.

عادات وممارسات الأفراد أو المجتمعات	
بعد دخول التقنية الرقمية	قبل دخول التقنية الرقمية

تأثير التحول الرقمي في تغيير مهن المستقبل

في ظل تسارع عجلة تغيير الحياة؛ ألقت التقنية الرقمية ظلالها على جانب كبير جداً في حياة الإنسان عامةً، وفي الجانب الوظيفي والمهني على وجه الخصوص، وبحث الإنسان سبل الاستفادة من التحول الرقمي المتسارع بمحاولة إدخال التقنية الرقمية لإنجاز الأعمال، وزيادة الإنتاج، وتوفير الجهد والتكلفة، للوصول إلى ازدهار الاقتصاد والنمو بشكل أسرع، وتطلب ذلك التكيف مع المتطلبات الحديثة، وتغيير المهن الحالية أو تحديثها، واستحداث مهن جديدة تواكب ذلك التحول.



نشر المنتدى الاقتصادي العالمي (World Economic Forum) في تقريره عن المهن المستقبلية (2020-2025م) بأن عدد (85) مليون وظيفة حالية يتوقع الاستغناء عنها، ويتوقع ظهور (97) مليون وظيفة لتلبية متطلبات التقنية المستقبلية،

وتتوقع الدراسات المستقبلية بأن هناك تغييراً في المهن الحالية ستكون من صالح الذكاء الاصطناعي ليحل بها محل الإنسان، ولهذا فإن المهن المستقبلية تتطلب مهارات تواكب احتياجاتها من قبل المهنيين، ومن هذه المهارات: الريادة، الإبداع والمبادرة، التفكير التحليلي والابتكاري، تحليل المعلومات، الذكاء العاطفي وغيرها من المهارات.

نشاط



1. ابحث عبر شبكة الإنترنت عن أهم (10) مهن مستقبلية في ظل التحول الرقمي، و (10) مهن مهددة بالاندثار.

م	المهن المستقبلية	م	المهن المهددة بالاندثار
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	

2. بين ما دورك العملي كطالب في السنة الأخيرة من المرحلة الثانوية عبر التهيئة والاستعداد لمواجهة مهن المستقبل في ظل التحول الرقمي.

1.
2.
3.
4.





يهدف برنامج تنمية القدرات البشرية الذي أطلقته المملكة العربية السعودية ضمن رؤية 2030 إلى إعداد المواطن المنافس عالمياً، والتركيز على مهارات القرن الحادي والعشرين، وغرس القيم والمعارف والمهارات اللازمة للمستقبل، لتطوير أساس تعليمي متين، والإعداد للسوق المستقبلي محلياً وعالمياً، وإتاحة فرصة التعلم مدى الحياة. يمكنك الاطلاع على البرنامج بمسح رمز الاستجابة السريع الظاهر.

إسهام العالم الرقمي في تعزيز التعليم وتطويره

أدى دخول التقنية في مجال التعليم إلى إنشاء المنصات التعليمية والتدريبية، والأدوات التقنية التعليمية المختلفة، وتطوير المقررات الرقمية، وأصبح بإمكان الأفراد التعلم في أي وقت، وفي أي مكان وفي ظل الظروف المختلفة، حيث أصبح التعلم جاذباً لكثير من الأفراد بشكل أسرع، وأكثر شمولاً، كما ساعدت بيئات التعلم الافتراضي ونظام التعليم عن بعد في إلحاق الطلاب بالتعليم النظامي عند تعذر تعلمهم حضورياً، لذا على المتعلم أن يمتلك المهارات الرقمية التي تجعله يواكب كل جديد، ومهارات القرن الحادي والعشرين التي تمكن الفرد بأن يكون متعلماً مدى الحياة.

نشاط



تحتوي شبكة الإنترنت على كثير من المنصات التعليمية والتدريبية المجانية أو المدفوعة والتي يمكن للطلاب الاستفادة منها في تطوير نفسه ومعارفه ومهاراته، قدّم تقريراً عن أشهر المنصات الرسمية المعروفة في شبكة الإنترنت العربية منها والأجنبية وفق الجدول الآتي:

م	المنصة	نوعها (تعليم/تدريب)	مجال المنصة	لغة التعلم (ع/ع)	الرسوم (مجاني/مدفوع)	إصدار شهادة (نعم/لا)
1						
2						
3						
4						
5						

منصات التدريب الرقمية لتطوير المهارات الوظيفية



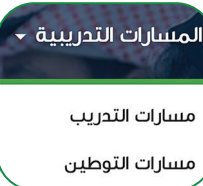
ضمن جهود حكومة المملكة العربية السعودية لتطوير مواطنيها؛ أنشئت منصة (دروب) التدريبية، وتعد منصة وطنية للتدريب الإلكتروني، وتتبع لصندوق تنمية الموارد البشرية "هدف"،

وتسعى إلى تطوير قدرات ورفع مهارات القوى الوطنية من الذكور والإناث، وإكسابهم المهارات الوظيفية التي تدعم حصولهم على الوظيفة المناسبة، والاستقرار بها وفق متطلبات سوق العمل السعودي، وتحتوي منصة "دروب" على العديد من البرامج التدريبية الإلكترونية، والمسارات التدريبية المجانية لموضوعات تدريبية متنوعة تلبي الاحتياجات الوظيفية. تتميز منصة دروب بمزايا عديدة، فهي تساعد على: تقديم دورات تدريبية لتحسين المهارات الوظيفية، والتأهيل للمنافسة في سوق العمل السعودي، وإكساب المعرفة والأدوات التي تساعد في إيجاد الوظيفة المناسبة، بالإضافة إلى منحها لشهادات معتمدة. يمكن الالتحاق بالمنصة والتسجيل بها عبر اتباع الخطوات الآتية:



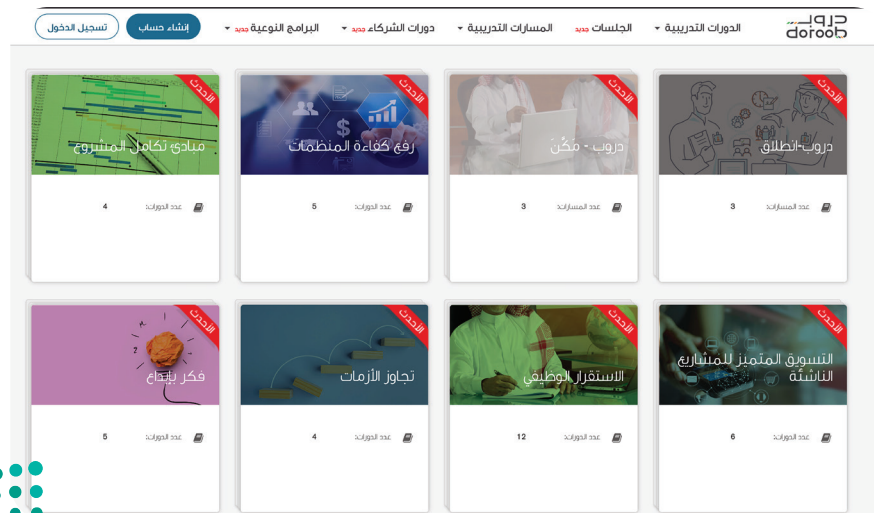
الخطوة الأولى: زيارة موقع المنصة عبر الرابط التالي: <https://doroob.sa/ar> أو بمسح رمز الوصول السريع.

الخطوة الثانية: أنشئ حساب بواسطة النقر على **إنشاء حساب** والدخول عبر "النفاذ الوطني"، يليها تعبئة البيانات الشخصية المطلوبة.



الخطوة الثالثة: اختيار أحد المسارات التدريبية المتوفرة كما في الشكل (1-5)، ومن ثم اختيار إحدى مجموعات الدورات بما يناسب الميول والاهتمامات لدى المتدرب، ويزيد من الخبرة والمهارة الشخصية، انظر شكل (1-6).

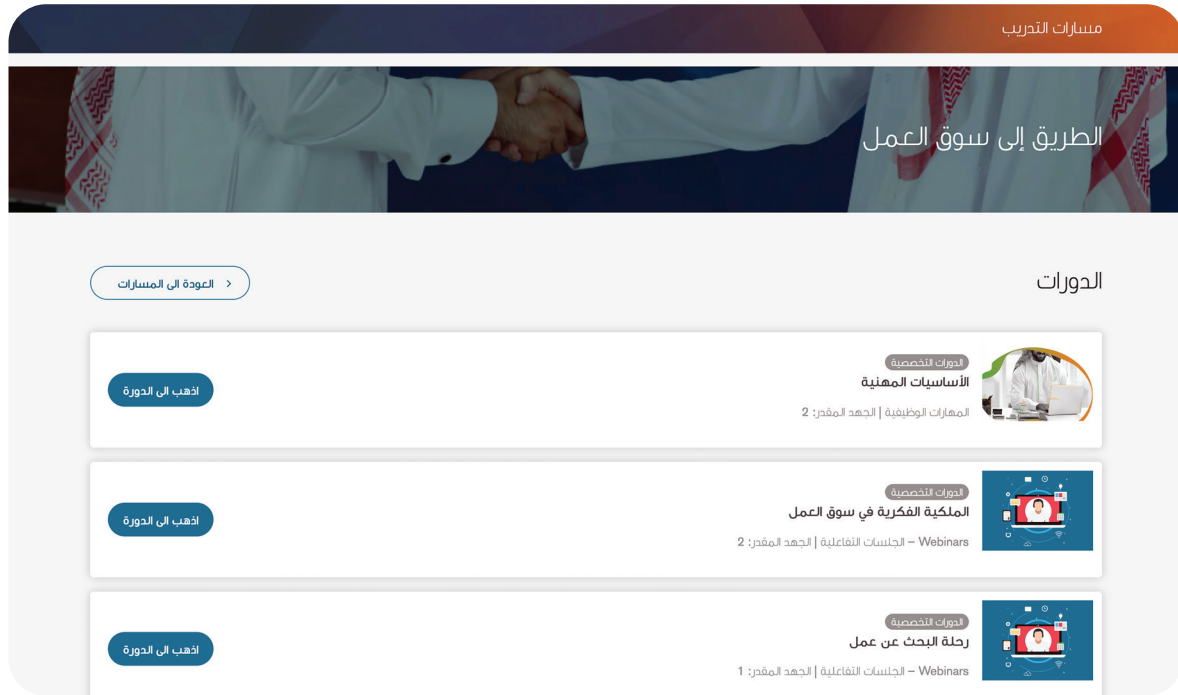
شكل (1-5): المسارات التدريبية



شكل (1-6): مثال على ظهور الدورات في المنصة

الخطوة الرابعة: بعد اختيار إحدى الدورات، تظهر صفحة الدورة التدريبية كما يظهر في الشكل (7-1)، وتتضمن زر التسجيل في الدورة التدريبية، ومعلومات تعريفية عنها يمكن من خلالها أخذ نبذة وافية عن الدورة قبل قرار الالتحاق بها، وتتضمن معلومات الدورة الآتي:

- اسم الدورة التدريبية.
- نبذة تعريفية عن الدورة التدريبية.
- هدف/أهداف الدورة التدريبية.
- الفئة المستهدفة.
- مستوى التعلم.
- المتطلبات السابقة - إن وجدت.
- متطلبات اجتياز الدورة التدريبية للحصول على الشهادة.



شكل (7-1): الصفحة التعريفية للدورة التدريبية المختارة

الخطوة الخامسة: بعد الالتحاق بالدورة عبر النقر على زر (سجل الآن) كما يظهر في الشكل (7-1) أعلاه، ستظهر الصفحة الخاصة بمتطلبات اجتياز الدورة، والمواصفات الفنية لجهازك، ودليل إرشادي مرئي لكيفية طباعة شهادة الدورة التدريبية، إضافة إلى زر (ابدأ الدورة) الذي يدخلك إلى محتوى الدورة مباشرة.





بعض الدورات التدريبية تتطلب إجراء (تقييم قبلي) قبل الدخول للدورة، و(تقييم بعدي) بعد الانتهاء منها لمقارنة مستوى إتقان المتدرب لمحتويات الدورة.



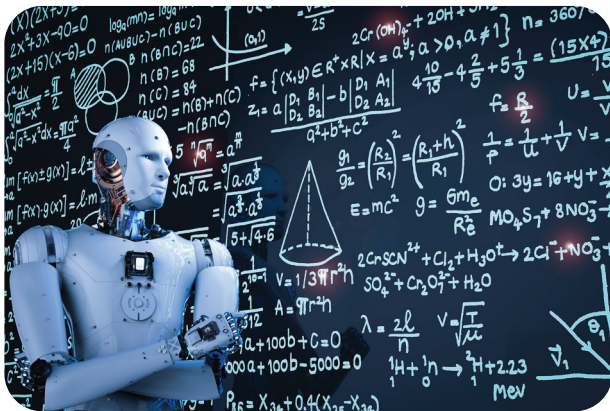
تقدم معظم المنصات التدريبية شهادات بعد إتمام الدورات يمكن أن تبني بها سيرتك الذاتية، وتكون داعمة لك في البحث عن الوظائف. لذا احرص أن تكون الدورات التدريبية تخدمك في مهن المستقبل كما درست.

تدريب



بناءً على خطوات الالتحاق بمنصة دروب التدريبية، نسّق مع معلّمك حول البحث عن إحدى الدورات التدريبية التي تناسب ميولك واهتماماتك عبر الالتحاق بها، وقدم الشهادة التدريبية للمعلّم بعد الانتهاء من الدورة التدريبية.

دور الذكاء الاصطناعي والبيانات الضخمة في تنمية المجتمعات



في العصر الحاضر لا يسعّ التحدث عن مدى تأثير العالم الرقمي على المجتمعات والأفراد دون الإشارة إلى الذكاء الاصطناعي والبيانات الضخمة ودورهما الكبير لتغيير دفة التحول الرقمي في تقديم الخدمات، والتنبؤ بالأزمات، وتحسين ابتكار الأعمال والمنتجات. يعرف الذكاء الاصطناعي (Artificial Intelligence) بأنه نظام حاسوبي يمكنه محاكاة عمليات الذكاء البشري كالنّعم، والاستدلال،

والتصحيح الذاتي، بينما البيانات الضخمة (Big Data) هي مجموعات البيانات الهائلة والمعقدة التي أتاحت من خلال الرقمنة (digitization)، والتي لا يمكن معالجتها، وتحليلها من خلال التقنيات التقليدية لمعالجة البيانات.



يقصد بمفهوم الرقمنة (Digitization) بأنها عملية تحويل المعلومات إلى تنسيق رقمي يمكن قراءته بواسطة الحاسوب، وذلك بهدف تمثيل صورة أو صوت أو مستند أو إشارة عن طريق توليد سلسلة من البيانات الرقمية بصيغة أرقام ثنائية يمكن لأجهزة الحاسوب معالجتها، وتسمى عملية التحويل بالتمثيل الرقمي دون إجراء أي تعديل في المحتوى الأساسي.

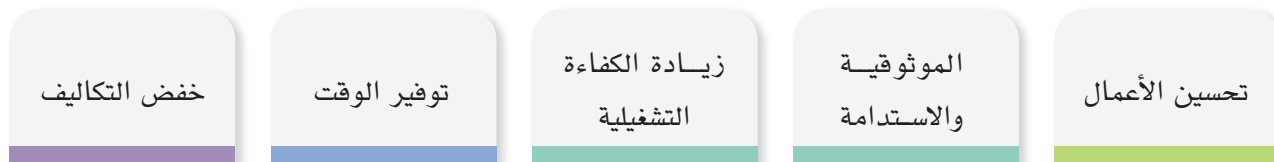
للاستفادة من البيانات الضخمة يجب إخضاعها لتحليلات حاسوبية متقدمة باستخدام الذكاء الاصطناعي وهما متكاملان، فالبيانات الضخمة غير مستغلة بدون حلول الذكاء الاصطناعي، ولا يمكن نشر حلول الذكاء الاصطناعي بنجاح بدون بيانات ضخمة، والتكامل بينهما يساعد في حل كثيرٍ من المشكلات المعقدة، ويوضح الشكل (8-1) مجموعة من التطبيقات التي يساعدان الذكاء الاصطناعي والبيانات الضخمة في حلها.

التعليم	الصحة	الملاحة الجوية
• تصنيف الطلاب بناء على نشاطاتهم المهارية. • الإجابة على استفسارات الطلاب في المواد الدراسية.	• مكافحة الأوبئة. • تشخيص الأمراض. • تطوير الأدوية.	• تحسين الخرائط. • تدفق الحركة المرورية. • التنبؤ بالأحوال الجوية.
الزراعة	الصناعة	البيئة
• الروبوتات الزراعية. • مراقبة المحاصيل والتربة. • مراقبة الآفات.	• تصميم المنتجات. • الروبوتات الصناعية. • الخدمات اللوجستية.	• مراقبة تلوث الهواء وانبعاثات الطاقة. • التنبؤ بالظروف الجوية والكوارث الطبيعية. • تحسين طرق توليد واستهلاك الطاقة. • مراقبة الغطاء النباتي.

شكل (8-1): تطبيقات الذكاء الاصطناعي والبيانات الضخمة في مجالات العمل



تشير التطبيقات في شكل (8-1) إلى بعض من التطبيقات الكثيرة والمتعددة والمتجددة من تكامل الاستفادة بين الذكاء الاصطناعي والبيانات الضخمة لتحسين جوانب الحياة المعاصرة، لذا تهدف تطبيقات الذكاء الاصطناعي والبيانات الضخمة إلى ما يأتي (الشكل 9-1):



شكل (9-1): الأهداف العامة لتطبيقات الذكاء الاصطناعي والبيانات الضخمة

تعد البيانات (Data) في العصر الحاضر من الموارد الأكثر قيمة حول العالم، وتتنافس عليها الدول والشركات لإعادة إنتاج بيانات جديدة تسهم في زيادة الإنتاج.  إضاءة

يتوقع أن يسهم الذكاء الاصطناعي بما يصل إلى 15.7 تريليون دولار في الاقتصاد العالمي بحلول 2030م، وهو أكثر من الناتج المحلي للصين والهند مجتمعين (itu.int).  إضاءة

غذاء الفكر

- هل يمكن التحضير لوظائف الغد باستخدام أدوات التعلم الماضية؟
- هل يوجد مهارات مستقبلية غير ما ذكر في الدرس؟
- لماذا تغيرت طريقة التواصل المعتادة بين الأشخاص من اتصال مباشر إلى إرسال الرسائل النصية أو الصوتية؟
- لماذا يفضل بعض الناس أداء الأنشطة الحياتية افتراضياً بدلاً من الأسلوب الواقعي المعتاد؟
- كيف يساعد تبني قنوات إعلامية رقمية رسمية على نشر الثقافة والهوية الإسلامية؟



- يكمن دور المواطن الرقمي المسلم في إبراز صورة الدين الإسلامي لدى الثقافات الأخرى بما يعكس صورته الحقيقية .
- يوجد فرق بين الرقمنة والتحول الرقمي، فالأول يقصد به تحويل المعلومات الواقعية بصيغة مستند رقمي في جهاز الحاسوب، أما التحول الرقمي فهو تغيير العمليات، وتحويل الأعمال بطريقة يتم تمكينها بواسطة الرقمنة، بحيث يتم الاستفادة من المعرفة ودمجها في مجالات الأعمال لتعزيز المشاركة وبناء قيمة جديدة.



مشروع الدرس



الموضوع:

تتعدد فوائد استخدام الذكاء الاصطناعي والبيانات الضخمة في مجالات الحياة المختلفة، بالتعاون مع أفراد مجموعتك وبالرجوع إلى مصادر المعلومات المتعددة، نفذ المشروع الآتي:

- اذكر استخدامات الذكاء الاصطناعي التي تخدم عمليتي التعليم والتدريب.
- بيّن مدى أهمية تطبيق الذكاء الاصطناعي والبيانات الضخمة في التعليم والتدريب.
- ناقش مدى ارتباط ما توصلت إليه في عملية البحث من الاستخدامات بالمهن المستقبلية في مجال الذكاء الاصطناعي.

الهدف: تقرير مجتمعي-مدرسي.

طريقة التنفيذ:

- تقسيم الطلاب إلى مجموعات.
- تنقسم عناصر المجموعة الواحدة إلى فريقين:
 - الفريق الأول: يتولى عملية البحث في المصادر المختلفة.
 - الفريق الثاني: يتولى تصميم العمل على هيئة رسم معلوماتي (Infographic) بواسطة إحدى أدوات التصميم المتاحة.

طريقة التقديم:

- طباعة التصميم على مقاس A0، وتثبيته على إحدى لوحات المدرسة.
- رفع التصميم على مدونة المادة.





الخدمات الرقمية

الدرس الثالث

مخرجات التعلم:



- أتعرف على مفهوم الخدمات الرقمية وأهم مميزاتها.
- أقترح بعض التطبيقات الرقمية التي يمكن أن تسهم في خدمة المجتمع.
- أتمكن من التعامل مع إحدى منصات الخدمات الحكومية الرقمية بمهارة.
- أناقش دور الخدمات الحكومية الإلكترونية في رفع مستوى رفاهية المواطن والمقيم.
- أستخدم بعض التطبيقات الحكومية الإلكترونية.
- أعد تقريراً عن أهم الخدمات والمشاريع الحكومية الإلكترونية.

مصطلحات الدرس:

- الخدمات الرقمية (Digital Services).
- المنصة الوطنية الموحدة (Unified National Platform).

التهيئة

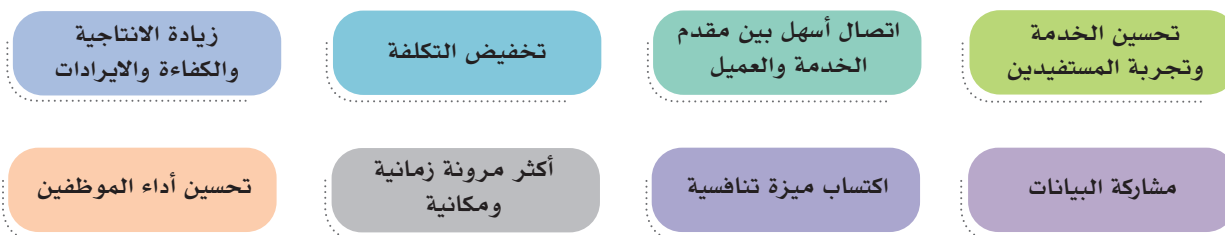
قبل البدء باستعراض فقرات الدرس ... فكّر في الأسئلة الآتية:

- كيف استخرجت بطاقة الهوية الوطنية الخاصة بك؟
- ما الطريقة التي يجدد بها والديك جواز السفر؟
- ما الخدمات الإلكترونية التي تستخدمها بشكل مستمر؟
- بعد التخرج، كيف يمكنك التقديم على الجامعات؟
- هل سبق لك تجربة التشخيص الطبي عن بعد عبر اتصال مرئي بينك وبين طبيبك؟
- ما المنصة التي استخدمتها للتقديم على اختبارات القدرات والتحصيلي؟ وكيف كانت تجربتك مع المنصة؟

الخدمات الرقمية

في وقتنا الحاضر تهدف الحكومات والشركات والمؤسسات حول العالم إلى التميز والتطور وتحسين جودة منتجاتها ومستوى خدماتها، وتؤدي الخدمات الرقمية دوراً بارزاً في تحقيق ذلك، وتماشياً مع رؤية 2030 وضمن برنامج التحول الوطني؛ سعت المملكة العربية السعودية إلى تنفيذ إستراتيجية التحول الرقمي بهدف توفير جميع الخدمات الحكومية رقمياً، وإتاحة الوصول إليها بسهولة. ويشير مفهوم الخدمات الرقمية (Digital Services) إلى الأعمال والخدمات التي

يتم تقديمها بواسطة تقنيات الاتصال والمعلومات، وكما يظهر في الشكل (10-1) فإن من أهم مميزات الخدمات الرقمية أنها تساعد في:



شكل (10-1): مميزات الخدمات الرقمية

نشاط



1. مع زيادة جودة وتحسين مستوى الخدمات الرقمية، حرص العديد من رواد الأعمال على تطوير خدمات رقمية تلبي حاجات المجتمع، اذكر اثنين من التطبيقات التي استخدمتها (حجز فنادق، تذاكر، طلبات طعام، مشتريات) مع توضيح الآتي:

اسم التطبيق	نوع الخدمة التي يقدمها	تقييمك للتطبيق



2. ما أبرز مميزات وعيوب تطبيقات الخدمات الرقمية؟

مميزات (غير المذكورة في الدرس)	عيوب

3. اقترح تطبيقاً رقمياً يمكن أن يقدم خدمة يحتاجها المجتمع.

الخدمات الحكومية الرقمية:

نشاط



تابع المادة المرئية عبر مسح رمز الاستجابة السريع ثم استخلص بعض الخدمات الحكومية الرقمية.



وزارة التعليم

Ministry of Education

2023 - 1445

أحرزت حكومة المملكة العربية السعودية تقدّمًا كبيرًا في أتمتة خدماتها، حيث إن 98% من الخدمات الحكومية تم تحويلها إلى خدمات إلكترونية، فقد حرصت العديد من الوزارات، والإمارات، والقطاعات الصحية والتعليمية، وغيرها من الجهات على تحويل خدماتها لتكون إلكترونية، هذا وقد حققت المملكة العربية السعودية المرتبة الأولى في مؤشر مستوى نضج خدماتها الحكومية على مستوى الشرق الأوسط وشمال أفريقيا بحسب لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي آسيا "الإسكوا" (ESCWA) التابعة لمنظمة الأمم المتحدة (انظر الشكل 11-1).



شكل (11-1): ترتيب المملكة في مستوى نضج الخدمات الحكومية، المصدر: هيئة الحكومة الرقمية



أُنشئت هيئة الحكومة الرقمية بقرار مجلس الوزراء رقم (418) بتاريخ 9 مارس 2021 الموافق 25 رجب 1442 هـ وهي الجهة المختصة بكل ما يتعلق بالخدمات الحكومية الرقمية، وتعد المرجع الوطني في شؤونها، وتهدف إلى تنظيم أعمال الحكومة الرقمية في الجهات الحكومية، من أجل الوصول إلى حكومة رقمية استباقية ومُبادرة وقادرة على تقديم خدمات رقمية ذات كفاءة عالية، وتحقيق التكامل في مجال الحكومة الرقمية بين كافة الجهات الحكومية، وللإطلاع على تفاصيل أهداف الهيئة وخدماتها، قم بمسح رمز الاستجابة السريع.



من أهم منصات الخدمات الإلكترونية الحكومية "المنصة الوطنية الموحدة" (Unified National Platform) وهي منصة رقمية متكاملة تقدم كافة الخدمات الحكومية بجودة وكفاءة عالية، عبر تجربة موحدة من خلال قنوات متعددة، تقدم الخدمات للمواطنين والمقيمين والزوار وأصحاب الأعمال التجارية.



زُر الموقع الإلكتروني للمنصة الوطنية الموحدة عبر مسح رمز الاستجابة السريع، ثم وضح في الجدول المرفق ثلاث من الخدمات التي توفرها المنصة.

اسم الخدمة	مميزات الخدمة



كيف يمكن أن يسهم التحول إلى الخدمات الرقمية في تطوير مستوى الخدمات الحكومية؟



تقدم العديد من الجهات الحكومية مجموعة واسعة من الخدمات الإلكترونية؛ وللإطلاع على معلومات أكثر حول هذه الجهات وخدماتها امسح رمز الاستجابة السريع، حيث يمكن الاطلاع على الموقع الإلكتروني للجهة ومعلومات الاتصال وموقعها على الخريطة وحساباتها على مواقع التواصل الاجتماعي، ويمكن عن طريق صفحة الجهة في الدليل الدخول إلى خدماتها الإلكترونية والاستفادة منها.

نشاط



12-1

بعد تسجيل الدخول الى حسابك في منصة أبشر، قم بالآتي:

1. تحدّث عن اثنين من الخدمات الحكومية الرقمية التي سهّلت منصة أبشر الحصول عليها.

اسم الخدمة	مميزات الخدمة

2. استخدم تطبيق أبشر للاستعلام عن:

- أحقيتك في الحج.
- تاريخ انتهاء جواز سفرك.

نشاط



13-1

ناقش الدور الذي قامت به الخدمات الحكومية الإلكترونية في زيادة رفاهية المواطن والمقيم، ثم لخص نتائج النقاش

مع مجموعتك.



- مع ارتفاع معدل التحول الرقمي، تبرز أهمية العناية بالأمن السيبراني فما السبب؟
- كيف يمكن أن تساعد الخدمات الرقمية في تقليل التكلفة؟
- ما دور الخدمات الرقمية في المحافظة على الاستدامة البيئية؟

- المدن الذكية هي أحد أشكال التحول الرقمي الذي تسعى حكومة المملكة العربية السعودية لتطويرها ومن أمثلتها مدينة نيوم، ومدينة ذا لاین.
- "آمر" خدمة إلكترونية تابعة لبرنامج "يسّر" متخصصة في الرد على استفسارات المواطنين والمقيمين ومساعدتهم في الاستفادة من الخدمات الحكومية الإلكترونية الأخرى.
- رضا المستفيد هو أحد الغايات الأساسية التي تسعى حكومة المملكة العربية السعودية لتحقيقها عبر التحول الرقمي، ولذلك من المهم أن تحرص على تقييم الخدمات المقدمة لمساعدة الحكومة في تجويد الخدمات.



مشروع الدرس



هناك العديد من المشاريع والخدمات الرقمية التي تقدمها حكومة المملكة العربية السعودية سعياً إلى رفع مستوى الخدمات المقدمة وزيادة رفاة المواطن والمقيم. بالاتفاق مع زملائك، اختر واحدة من هذه الخدمات أو المشاريع.

● قم بعمل بحث يشمل:

- التعريف بالخدمة / المشروع.
- أهداف الخدمة/ المشروع ومميزاته.
- معلومات إضافية حول الخدمة / المشروع.
- صمّم عرض يلخص أهم المعلومات.
- قدّم العرض أمام معلمك وزملائك في الفصل.





الوعي الإعلامي الرقمي

الدرس الرابع

مخرجات التعلم:

- أتعرف على مفهوم الوعي الإعلامي الرقمي وأميز أهم كفاياته المعرفية.
- أناقش مفهوم الإعلام الرقمي، وخصائصه، وأهم قنواته.
- أستنتج أهمية الإعلام الرقمي.
- أتعرف على مفهوم مهارة القراءة الجانبية، وأهميتها.
- أطبق خطوات مهارة القراءة الجانبية للتحقق من صحة المادة الإعلامية الرقمية.
- أتعرف على مفهوم إعلام المواطن، ووسائله، وخصائصه.
- أستنتج فوائد وعيوب إعلام المواطن.
- أنتج مادة إعلامية رقمية ألتزم بها بقوانين نظام المطبوعات والنشر في المملكة العربية السعودية.



مصطلحات الدرس:

- الوعي الإعلامي الرقمي (Digital Media Literacy).
- الإعلام الرقمي (Digital Media).
- المعلومات المضللة (Disinformation).
- المعلومات الزائفة (Misinformation).
- القراءة الجانبية (Lateral Reading).
- إعلام المواطن (Citizen media).

التهيئة

لم تعد الصحف والمجلات والمحطات الإخبارية مصادر الإعلام الوحيدة في عصر الانفتاح الرقمي، بل تعددت المصادر والجهات لدرجة جعلت من الضروري أن يتعلم الأفراد كيفية التفكير بشكل ناقد فيما يرد على الأخبار ووسائل الإعلام الرقمي، فليس كل ما يعرض صحيح، والواجب على المؤمن الكيس الفطن والمواطن الرقمي الواعي أن يلاحظ، يفكر، يتحقق، يقيم أثناء قراءته للمواد الإعلامية أو إنتاجه لها، وهذا هو النهج الإسلامي، يقول الله تعالى: ﴿يَتَأَيَّهَا الَّذِينَ ءَامَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَأٍ

فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصْحِحُوا عَلَىٰ مَا فَعَلْتُمْ نَادِمِينَ﴾ [الحجرات : 6]

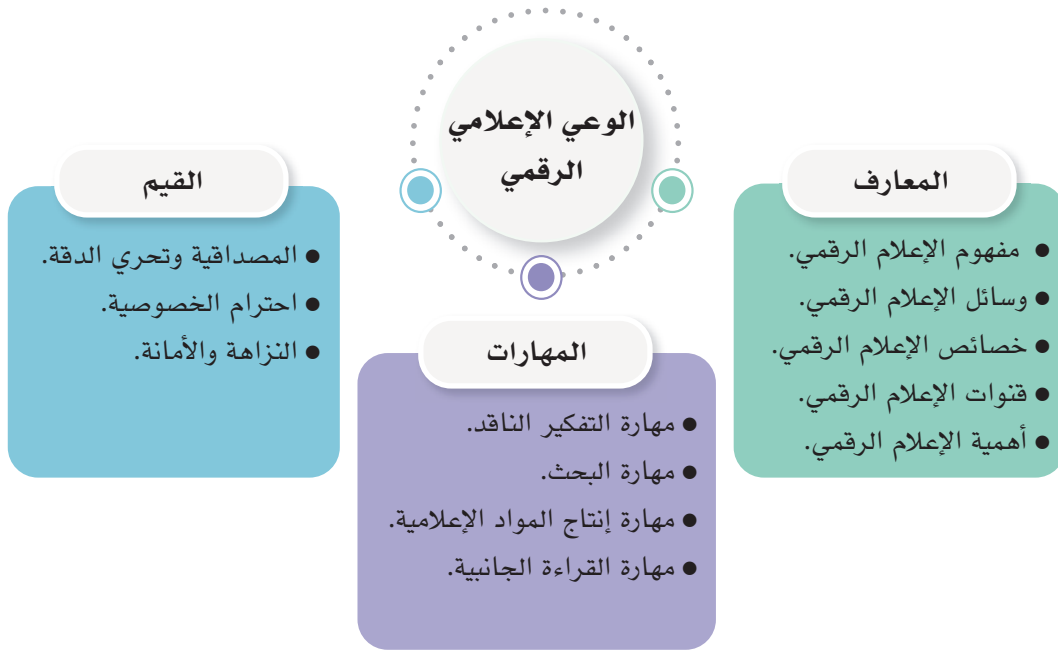
للتفكير:

- هل أنت مهتم بمتابعة المواد الإعلامية (المكتوبة أو المرئية أو المسموعة)؟
- ما نوع المواد الإعلامية التي تتابعها؟
- هل يعد سبقاً صحفياً عندما ينشر أي مواطن رقمي في فضاء مدونته أو حساباته مواد إعلامية قبل وسائل الإعلام التقليدية؟
- ما مسؤولياتك كمواطن رقمي مستهلك؟
- ما مسؤولياتك كمواطن منتج للمواد الإعلامية؟



|| الوعي الإعلامي الرقمي

أصبحت المواد الإعلامية الرقمية متوفرة في كافة الأجهزة الرقمية، ويمكن للمستخدم الوصول لها في أي وقت، وهذا الانفتاح الإعلامي جلب معه العديد من الإيجابيات والسلبيات التي شكّلت أهمية التوعية وتطوير المهارات في طريقة إنتاج واستهلاك المواد الإعلامية، ومن هذا المنطلق ظهر الوعي الإعلامي الرقمي (Digital Media Literacy) ويقصد به: القدرة على البحث والوصول للمواد الإعلامية وتحليلها وتنظيمها وتقييمها، وإعادة استخدامها أو إنتاجها، وعلى الأخص في المواقف التي تتطلب اتخاذ قرار أو حل مشكلة أو اكتساب معرفة. يوضح الشكل (1-12) كفايات الوعي الإعلامي الرقمي (المعارف، والمهارات، والقيم) التي ينبغي أن يطورها المواطن الرقمي ليمتلك الوعي الإعلامي الرقمي:



شكل (1-12): كفايات الوعي الإعلامي الرقمي

|| البعد المعرفي في الوعي الإعلامي الرقمي

يشير مفهوم الإعلام الرقمي (Digital media) إلى الإعلام الذي يعتمد على استخدام الإنترنت والأجهزة الإلكترونية والوسائط الرقمية لنقل المادة الإعلامية والاتصال بالجمهور، حيث يمكن إنشاء المواد الإعلامية سواء كانت مسموعة أو مرئية أو مقروءة وتعديلها ونشرها وتوزيعها من خلال التقنية الرقمية. تتنوع مجالات محتوى الإعلام الرقمي، فقد تكون

مواد إخبارية، أو ترفيهية، أو رياضية، أو دعائية وغيرها من المجالات، كما تتعدد الوسائل الإعلامية الرقمية والتي يمكن الوصول لها من خلال الهواتف الذكية أو أجهزة الحاسوب ومنها:

- التطبيقات الرقمية.
- وسائل التواصل الاجتماعي.
- مواقع ومنتديات الإنترنت المسموعة والمرئية والمقروءة.
- الألعاب الرقمية.
- تقنيات الواقع الافتراضي والواقع المعزز.
- الصحف الإلكترونية.
- تلفزيون الإنترنت.
- الإذاعات الرقمية.
- المجموعات البريدية.

|| خصائص الإعلام الرقمي

يتميز الإعلام الرقمي بمجموعة من الخصائص موضحة في الشكل (13-1):



شكل (13-1): خصائص الإعلام الرقمي



يعد تخصص «الإعلام الرقمي» من التخصصات الدراسية التي ظهرت مع التطور الرقمي، ويتيح للخريجين شغل العديد من الوظائف، منها على سبيل المثال لا الحصر:

- مطور مواد إعلانية رقمية.
- محرر صحفي رقمي.
- متخصص في صناعة الرسوم والوسائط المتحركة.
- مصمم مواد بصرية.
- منتج رقمي.
- إدارة محتوى رقمي.
- أكاديمي متخصص في الإعلام الرقمي.
- مطور مواقع ويب إخبارية.



قنوات الإعلام الرقمي

يوضح الشكل (1-14) أربعة أنواع من قنوات الإعلام الرقمي:



شكل (1-14): قنوات الإعلام الرقمي



بعد الاطلاع على الخصائص التي يتميز بها الإعلام الرقمي وقنواته، استنتج أهمية الإعلام الرقمي ولماذا يعد قوة مؤثرة؟

|| أهمية الإعلام الرقمي

للإعلام الرقمي تأثير مهم في توجيه اهتمامات الناس وسلوكهم وطريقة تفكيرهم، كما يعد قوة مؤثرة في توجيه الرأي العام وذلك للأسباب الآتية:

1. مناسبه لمختلف فئات المجتمع بسبب تقديم المادة الإعلامية بأكثر من طريقة عبر مختلف قنوات ووسائل الإعلام الرقمي.
2. الوصول لأكبر فئة من الجمهور العالمي حيث إنه غير مرتبط بنطاق جغرافي معين أو بلغة معينة مما يساعد على نشر المادة الإعلامية وترجمتها للعديد من اللغات.
3. التكتيف الإعلامي من خلال استمرار عرض المادة الإعلامية مما يجعل تأثيرها أعلى على الجمهور.
4. يحظى الإعلام الرقمي بنوع من المصادقية عند الجمهور بسبب تنوع قنواته حيث إن المادة الإعلامية لم تعد حكراً لجهة معينة.
5. التحديث المستمر وإمكانية الوصول المباشر للمواد الإعلامية مما يبقي الجمهور على إطلاع مستمر بالمستجدات.
6. تخصيص تجربة المستخدم حيث يمكن للمتلقي اختيار المادة الإعلامية التي تناسبه.
7. المشاركة في صنع المادة الإعلامية من خلال النشر أو الرد والتعليق وإبداء الرأي.

البعد المهاري في الوعي الإعلامي الرقمي

هناك كم هائل من المواد الإعلامية الرقمية مما يجعل من السهل تمرير معلومات مغلوطة، وهي على نوعين:

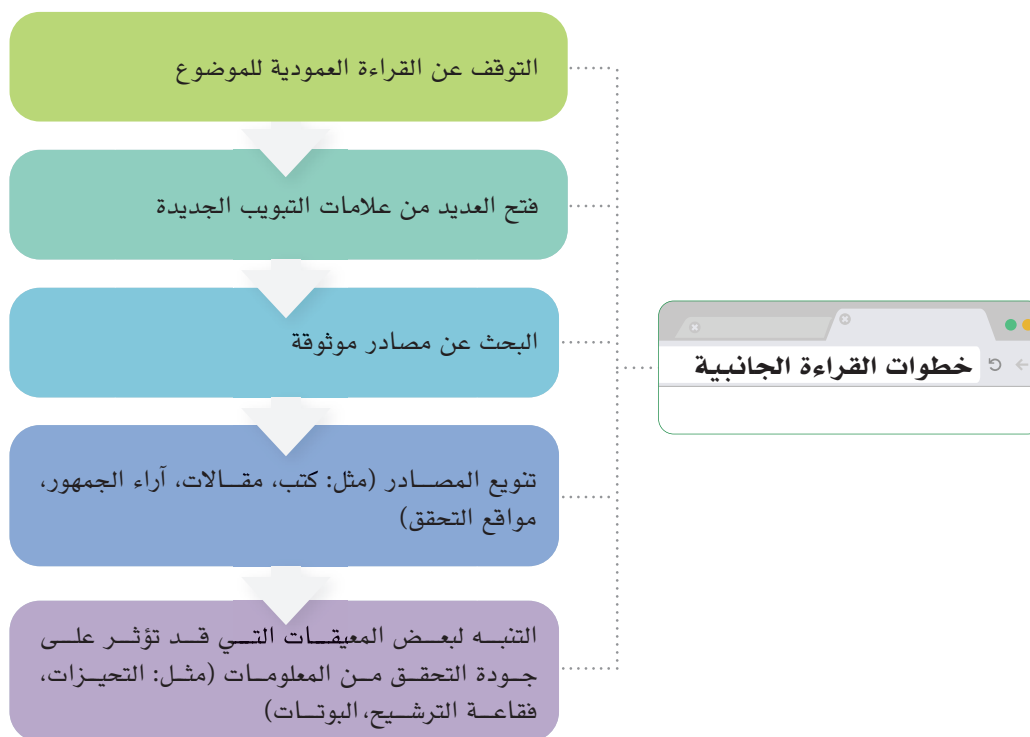
- المعلومات المضللة (Disinformation): معلومات غير صحيحة يتم نشرها عمداً بهدف تضليل الجمهور أو توجيههم.



- المعلومات الزائفة (Misinformation): المعلومات التي تحتوي على عناصر من الحقيقة، ولكنها غير دقيقة في مجملها والمنتشرة عبر الإنترنت دون هدف مقصود للتضليل أو التلاعب بالجمهور.

ولهذا من المهم أن يكون لدى المواطن الرقمي بعض المهارات التي تساعد على التفكير الناقد في المحتوى الإعلامي وتحليله وتقييم مدى صحته، وضمان الاستفادة الصحيحة من المعلومات المطروحة، ومن أهم هذه المهارات "مهارة القراءة الجانبية (Lateral Reading)" التي يقصد بها تقييم مصداقية المادة الإعلامية من خلال مقارنتها بمصادر أخرى وهي من المهارات الفعالة التي تساعد على تمييز المعلومات المغلوطة من المعلومات الموثوقة سواء كانت المعلومات نصية أو مقاطع مرئية أو مسموعة، ومن فوائدها:

1. التحقق من الأدلة.
 2. وضع المعلومات في سياقها (من الذي يقف خلف المعلومة وما دوافعه).
 3. البحث عن نقاط الضعف المحتملة.
- وللقيام بذلك اتبع الخطوات الموضحة بالشكل (1-15):



شكل (1-15): خطوات القراءة الجانبية





تساعد القراءة الجانبية الشخص في التحول من التلقي السلبي للمواد الإعلامية إلى مفكر وناقد من خلال التحقق وفحص المعرفة (Fact Check). يوضح الشكل (16-1) الأسئلة الرئيسة التي يسألها المواطن الرقمي الواعي ويبحث عن إجابات لها:

الهدف:	المصادقية:	المصدر:
ما الغاية من نشر المعلومة؟	ما الأدلة الداعمة للمعلومة؟	من يقف خلف المعلومة؟
من الجمهور المقصود؟ ولماذا؟ ما الرسالة التي يرغب المؤلف بتوصيلها؟ وهل هناك دافع خلف الرسالة؟ (اقتصادي، سياسي، شخصي، ديني، توعوي)	ما مدى حداثة الموقع / المقالة؟ متى تم نشره أو آخر تحديث له؟ ما تقييم المواقع الأخرى عن المؤلف أو الموقع؟ ما المصادر الأخرى للتحقق من المعلومة؟	من المؤلف؟ ما الموقع الناشر للخبر؟ ماذا يمكن أن أعرف عن المؤلف؟ ما التحيزات التي قد تكون لدى المؤلف؟

شكل (16-1): أسئلة مهارة القراءة الجانبية

أثناء التحقق من صحة المعلومات يجب الحذر من الانحياز التأكيدي (Confirmation bias) وهو عملية انتقاء معرفي يميل فيها الشخص للبحث عن المعلومات والتفسيرات التي تتوافق مع معتقداته وافتراضاته سواء كان ذلك بقصد أو دون قصد.



عند التحقق من صحة المادة الإعلامية بالإمكان البحث في:

- موقع مصدر الخبر الأصلي.
- الصحف الإلكترونية المعروفة.
- الحسابات الإلكترونية الإخبارية الموثوقة.
- الحسابات الإلكترونية الحكومية.
- مواقع خاصة تقوم بمهمة المحقق المعرفي.
- البحث باسم المؤلف.



إثارة التفكير:



ما رأيك في «ويكيبيديا» كمصدر للتحقق من المعلومات؟

أثناء الاطلاع على المادة الإعلامية أو التحقق منها، لابد من الانتباه إلى بعض تقنيات الذكاء الاصطناعي التي قد تؤثر على جودة البحث، ومنها:

- فقاعة الترشيح (Filter bubble): خوارزميات تستخدمها محركات البحث ووسائل التواصل الاجتماعي تحدد نتائج البحث التي تظهر للمستخدم وفق تفضيلاته السابقة.
- بوتات الإنترنت (Internet Bots): روبوتات تحمل خوارزميات تحاكي السلوك البشري في الإنترنت قد تكون نافعة أو ضارة؛ تستخدم البوتات في وسائل التواصل الاجتماعي ويمكن أن تقوم بإنتاج ونشر أخبار كاذبة على نطاق واسع، والقيام بهجمات على بعض الحسابات، زيادة عدد المتابعين لأهداف غالباً ما تكون اقتصادية أو سياسية.
- تقنية التزييف العميق (Deep fake): مقاطع مرئية (videos) مزيفة يتم إنشاؤها باستخدام البرامج الرقمية والتعلم الآلي ومبادلة الوجوه، حيث بإمكان هذه التقنية أن تنتج مقاطع مصورة لم تحدث على أرض الواقع بهدف التضليل.



إضاءة

نشاط



15-1

طبّق مهارة القراءة الجانبية للتحقق من صحة خبر اطلعت عليه عبر أحد وسائل التواصل الاجتماعي.

مصدر الخبر:

.....

نص الخبر:

.....



الهدف: الغاية من نشر الخبر	الأدلة الداعمة لصحة المصادر	ابحث عن مصادر إضافية للتحقق من صحة الخبر (4 مصادر على الأقل)
التقييم للخبر (القصة)		
غير صحيح		صحيح

إعلام المواطن

مع توفر التقنية الرقمية الحديثة أصبح بإمكان أي شخص أن يكتب ويصور وينشر عبر شبكة الإنترنت، ومن ذلك ظهر مفهوم "صحافة المواطن" أو "إعلام المواطن" (Citizen Media) وهو إعلام يصنعه أو يشارك في صنعه المواطن بحيث يوظف وسائل التقنية الرقمية من أجل صناعة المواد الإعلامية.

وسائل إعلام المواطن

يمكن للمواطن الإعلامي أن يقوم بالآتي:

- النشر النصي والسمعي والمرئي: تقديم مواد إعلامية عبر المدونات، وشبكات التواصل الاجتماعي، ومواقع البث المرئي والسمعي.
- التعليق: كتابة التعليقات في المنتديات، والمجموعات الإخبارية، وشبكات التواصل الاجتماعي.
- التحرير: تسمح بعض المواقع بعملية التحرير الجماعي من خلال برمجيات الويكي (wiki) فيمكن للمواطن الإعلامي أن يعدل وينقح المحتوى.
- التأكد من الحقائق: التحقق من صحة المواد الإعلامية المنشورة وكتابة تقارير ونشرها.
- التغطية الإعلامية: أحد أهم وظائف إعلام المواطن حيث يقوم المواطن الموجود في موقع الحدث بتصويره وصناعة تقرير إخباري ونشره كسبق صحفي.



خصائص إعلام المواطن

يتميز إعلام المواطن بالعديد من الخصائص، ويوضح الشكل (17-1) أهم تلك الخصائص وهي:

الديموقراطية: يمكن لأي شخص المشاركة في صنع المادة الإعلامية فلم يعد الإعلام حكراً على فئة معينة.

غير ربحية: إعلام المواطن غير تابع لمؤسسات رسمية تسعى إلى الربح المادي من خلال الإعلام.

التزامنية: يمكن لإعلام المواطن أن يقوم بالتغطية المباشرة للأحداث بطريقة أسرع من الإعلام التقليدي.

الحرية: يوفر إعلام المواطن منصة للتعبير عن الرأي بدون الانتماء لجهة ذات توجهات معينة مما يعطي حرية في التعبير.

التشاركية: التحول من وسائل الإعلام الجماهيرية إلى إعلام الجماهير حيث إن المادة الإعلامية يتم إنتاجها من الجمهور وإلى الجمهور.

شكل (17-1): خصائص إعلام المواطن

نشاط



بعد الاطلاع على مفهوم إعلام المواطن ووسائله وخصائصه، استنتج أهم مميزاته وعيوبه.
ملاحظة: بالإمكان الاستعانة بمحررات البحث.

عيوب إعلام المواطن	مميزات إعلام المواطن

|| البعد القيمي للوعي الإعلامي الرقمي:

- على المواطن الرقمي الالتزام بعدد من القيم عند الرغبة في المساهمة بالإنتاج الإعلامي، ومن أهمها:
- المصداقية: يجب على المواطن الإعلامي الرقمي تحري الدقة والمصداقية قبل نشر المادة الإعلامية.
 - النزاهة والأمانة العلمية: الالتزام بالأمانة والنزاهة عند النقل من الآخرين من خلال الإشارة لمصادر المعلومات حيث إن الإخلال بذلك قد يعرض صاحبه للعقوبات بموجب حماية حقوق الملكية الفكرية (سيتم التطرق لنظام مكافحة جرائم المعلوماتية في الوحدة الثالثة).
 - الاحترام والمسؤولية: يجب احترام خصوصية الأفراد والمؤسسات والالتزام بالحدود النظامية والشرعية المحددة بموجب نظام المطبوعات والنشر في المملكة العربية السعودية الموضحة في الشكل (1-18) ونظام مكافحة جرائم المعلوماتية (سيتم الحديث عن الجرائم المعلوماتية في الوحدة الثالثة) والإخلال بذلك يعرض صاحبه للعقوبات.

بالرجوع إلى نظام المطبوعات والنشر في المملكة العربية السعودية، يوجد ما نصه:

المادة الثامنة: حرية التعبير عن الرأي مكفولة بمختلف وسائل النشر في نطاق الأحكام الشرعية والنظامية وتعرض المادة التاسعة شروطاً ضابطةً ترافق هذه الحرية، حيث ورد ما نصه: يحظر أن يُنشر بأي وسيلة كانت أي مما يأتي

- 1 ما يخالف أحكام الشريعة الإسلامية أو الأنظمة النافذة
- 2 ما يدعو إلى الإخلال بأمن البلاد أو نظامها العام، أو ما يخدم مصالح أجنبية تتعارض مع المصلحة الوطنية
- 3 التعرض أو المساس بالسمعة أو الكرامة أو التجريح أو الإساءة الشخصية إلى مفتي عام المملكة أو أعضاء هيئة كبار العلماء أو رجال الدولة
- 4 إثارة التفرقات وبعث الفرقة بين المواطنين
- 5 تشجيع الإجرام أو الحث عليه
- 6 ما يضر بالشأن العام في البلاد

شكل (1-18): محظورات النشر بحسب نظام المطبوعات والنشر في المملكة العربية السعودية





امسح رمز الاستجابة السريع للاطلاع على تفاصيل:

نظام المطبوعات والنشر بالمملكة العربية السعودية



اللائحة التنفيذية لنشاط النشر الإلكتروني

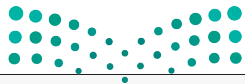


نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية



اقرأ الحالات الموضحة في الجدول أدناه، وحدّد ما إذا كانت المادة الإعلامية مناسبة للنشر مع تعليل الإجابة.

السيناريو	مناسبة / غير مناسبة للنشر	التعليل
تصوير مقطع لحادثة حصلت في أحد المطاعم حيث يظهر في التصوير وجوه بعض الأشخاص المتواجدين والمشاركين في الحادثة ونشرها على أحد وسائل التواصل الاجتماعي		
تسجيل مدونة صوتية (بودكاست) محتواها يركز على تحليل الوضع الاقتصادي في البلاد		
كتابة مقال نقدي عن الفساد الإداري مع ذكر الأسماء الصريحة لبعض المنظمات والأفراد		
عمل إعلان لمنتج ونشره على وسائل التواصل الاجتماعي بعد الحصول على تصريح لعمل الإعلانات.		





- لماذا تعدّ وسائل التواصل الاجتماعي ذات قوة ونفوذ في مجال الإعلام الرقمي؟
- ما عواقب انتشار الأخبار المضللة والزائفة على مستوى الأفراد والمؤسسات والحكومات؟



- لابد من التحقق من المواد الإعلامية المنتشرة وعدم تصديق كل ما يُنشر حيث يمكن لأي شخص النشر على الإنترنت ووسائل التواصل الاجتماعي دون الالتزام بأي معايير تحريرية، ناهيك عن التحقق من صحة المعلومات.
- يتم كتابة الأخبار المضللة ونشرها بقصد إلحاق الضرر بالمؤسسات، أو الأشخاص، أو لتحقيق مكاسب مالية، أو سياسية.
- يتم تصميم مواقع الويب الإخبارية الزائفة بطريقة احترازية يصعب كشفها في بعض الأحيان.
- يمكن تمييز الأخبار المغلوطة من خلال طريقة صياغة الخبر أو عنوانه حيث تميل لاستخدام عناوين مثيرة ومعلومات غير مدعومة بمصادر.



مشروع الدرس



بالتعاون مع زملائك، اختر خبراً من أخبار مدرستك لتغطيته باتباع الخطوات الآتية:

- حدد الموضوع أو الحدث المراد تغطيته، قد يكون مقابلة مع أحد المعلمين أو الزملاء الموهوبين أو لتغطية أحداث معرض في المدرسة.
- حدد المعايير الأخلاقية والمهارية التي يجب اتباعها لعمل هذا التقرير.
- اختر طريقة عمل التقرير، قد يكون تقرير نصي، أو مرئي أو صوتي.
- حدد المنصة الرقمية التي ترغب في استخدامها لنشر الخبر.
- قدّم عرضاً أمام المعلم والزملاء للمادة الإعلامية التي تم إعدادها.





www.ien.edu.sa

الوعي بالتعامل مع التجارة الإلكترونية

الدرس الخامس

مخرجات التعلم:



- أعرف مفهوم التجارة الإلكترونية.
- أطبق إرشادات الحماية لإنجاز المعاملات الرقمية المالية.
- أستشعر أهمية دور التجارة الإلكترونية في تحسين جودة الحياة.
- أمتلك المعرفة بالخطوات الآمنة للتسوق من المتاجر الإلكترونية.
- أستنتج فوائد تحول المستهلك العادي إلى مستهلك ذكي.
- أحدد خطوات بناء متجر إلكتروني.
- أستشعر أهمية الجهود المبذولة من المملكة العربية السعودية لتوفير تجارة رقمية آمنة.

مصطلحات الدرس:

- التجارة الإلكترونية (e-Commerce).
- التعاملات المالية الرقمية (Digital Financial Transactions).
- المتجر الإلكتروني (Online Store).
- التسوق الآمن عبر الإنترنت (Safe Online Shopping).

التهيئة

قبل البدء باستعراض محتويات الدرس ... فكّر في الأسئلة الآتية:

- هل قمت بعملية شراء إلكتروني بنفسك سابقاً؟ أو بإشراف أحد والديك؟
- ما الذي يميّز الشراء من متجر إلكتروني بدلاً من الذهاب إلى متجر محلي في مدينتك؟
- هل تثق في كل متجر متوفر عبر شبكة الإنترنت، وكيف تتحقق من موثوقية المتجر الإلكتروني الذي تتسوق منه؟
- كيف تعرف مواصفات المنتج الذي تريد شراءه؟ وكيف تتعامل مع المتجر بعد عملية الشراء.
- هل سبق أن طلبت من متجر إلكتروني ولم تحصل على الطلب رغم دفع المبلغ؟
- كيف تتسوق بأمان من المتاجر الإلكترونية؟
- هل فكرت في إنشاء متجر إلكتروني؟ وما الاشتراطات المطلوبة لذلك؟



|| مفهوم التجارة الإلكترونية (e-Commerce)

بيّن الله -سبحانه وتعالى- في القرآن أهمية البيع والشراء بما فيها من البحث عن رزق الإنسان، فقال -سبحانه وتعالى: ﴿وَأَحَلَّ اللَّهُ الْبَيْعَ وَحَرَّمَ الرِّبَا﴾ [البقرة: 275]، ودلّ القرآن الكريم كذلك على أهمية وضوح التعاملات المالية بين البشر، وتنظيم سلوكياتهم أثناء ممارسة التجارة، فقال -سبحانه وتعالى-: ﴿يَا أَيُّهَا الَّذِينَ ءَامَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَتْ تِجَارَةً عَنْ تَرَاضٍ مِّنْكُمْ﴾ [النساء: 29]

وفي العصر الحديث ظهر مفهوم جديد للتجارة يتيح للتاجر والمتسوق بيع وشراء البضائع، وإجراء الخدمات المالية بطريقة أكثر تطوراً، وبدون قطع المسافات، وعبر أسواق بعيدة (متاجر افتراضية) وهي ما يطلق عليه حالياً بالتجارة الإلكترونية (e-Commerce) التي تعرف بأنها: نشاط ذو طابع اقتصادي يباشره موفر الخدمة والمستهلك بوسيلة إلكترونية من أجل بيع، أو تقديم خدمات، أو الإعلان عنها، أو تبادل البيانات الخاصة بها.



نشاط



شارك خبرتك السابقة مع زملائك بعمليات شراء أو بيع مارستها سابقاً عبر شبكة الإنترنت، واذكر الفوائد التي تعلمتها من هذه التجربة.



تنبع أهمية التجارة الإلكترونية للمواطن الرقمي بالتعلم كيف يكون مستهلكاً ذكياً في اختيار المنتجات، وكيف يجري عمليات الشراء الآمنة عبر شبكة الإنترنت، ومعرفة المواقع الموثوقة والأمنة، ومعرفة الحقوق التي يتمتع بها المتسوق الإلكتروني للاستفادة من الخدمات المتاحة، وتقديم النصائح للآخرين كتجنب عمليات الاحتيال، وسرقة الهوية، والمحافظة على البطاقات الائتمانية والحسابات البنكية.

نشاط جماعي



عدد مع زملائك بعضاً من مواصفات المنتجات التي ترون أفضلية شرائها من شبكة الإنترنت بدلاً من المتجر المحلي؟ ولماذا ترى ذلك.



وزارة التعليم

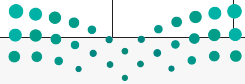
Ministry of Education

2023 - 1445

أكمل الاستبيان الحالي، وشارك مجموع النتيجة النهائية مع زملائك حسب التقييم الآتي:

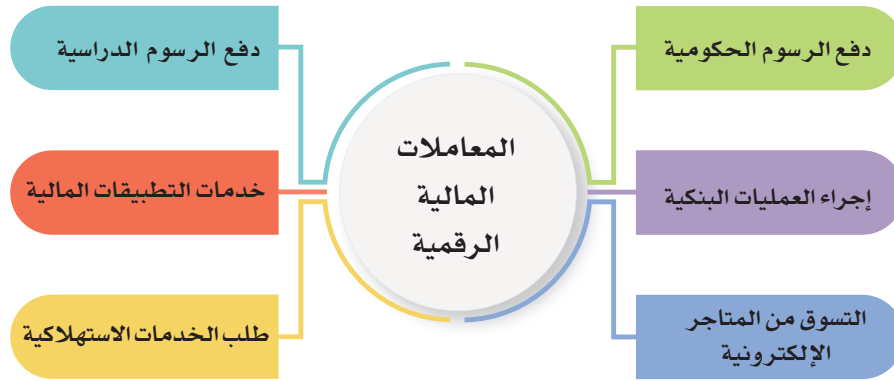
- متسوق رقمي متمكن (28 إلى 36).
- متسوق رقمي متوسط التمكن (14 إلى أقل من 28).
- متسوق رقمي غير متمكن (أقل من 14).

م	الممارسة	دائمًا (3)	أحيانًا (2)	أبدًا (1)
1	اشترت سابقاً من شبكة الإنترنت.			
2	أنفقت مبالغ كبيرة في عملية الشراء عبر شبكة الإنترنت.			
3	بعت ممتلكات لدي عبر شبكة الإنترنت.			
4	أمضي بعضاً من الوقت في البحث والقراءة عن وصف المنتجات قبل الشراء.			
5	أتحقق من المتجر الإلكتروني قبل البحث عن المنتجات التي بداخله.			
6	أقرأ تقييم العملاء الذين اشتروا المنتج سابقاً.			
7	أضع منتجات في قائمة الرغبات (سلة الشراء) للتفكير بها لفترة من الزمن قبل الإتمام النهائي لعملية الشراء.			
8	استخدم وسائل الدفع الإلكترونية مثل الباي بال (pay-pal).			
9	أجرى تعاملاتي المالية عبر التطبيقات الذكية.			
10	أشحن بطاقة الشراء عبر المتجر الإلكتروني لحسابي البنكي.			
11	أجريت عمليات شراء من خلال أنظمة الألعاب المختلفة.			
12	أتتبع البضاعة التي اشتريتها عبر شركة الشحن.			



إرشادات الحماية لإنجاز المعاملات المالية الرقمية

تتنافس كثيرٌ من الجهات الحكومية والتجارية في تقديم المعاملات المالية الرقمية (Digital Financial Transactions) مواكبة للتطور الذي يشهده التقدم الرقمي في الوقت الحالي، وتعد الخدمات المالية من الوسائل المريحة للأفراد لإنجاز معاملاتهم المالية الدائمة والملحة، كما أنها دلالة واضحة للمستوى الذي وصل إليه الأفراد في ممارستهم الرقمية. تتنوع المعاملات المالية الرقمية التي يمارسها الأفراد حسب احتياجاتهم اليومية كما يوضحها الشكل (19-1) الآتي:



شكل (19-1): بعض المعاملات المالية الرقمية اليومية للأفراد

لذا يوجد العديد من الإرشادات الواجب على المواطن الرقمي اتباعها عند التعامل بالمعاملات المالية الرقمية، والتي ترفع من مستوى وعيه أثناء التعامل بالتقنية الرقمية، وتضعه في مأمن من عمليات الاحتيال المتنوعة، والمتجددة بشكل دوري، ويتمكن من البقاء آمناً لحفظ هويته وممتلكاته، ومن هذه الإرشادات:

- الدخول إلى الموقع الرسمي لمقدم الخدمة الإلكترونية المالية (لماذا؟).
- تحميل التطبيق الرسمي لمقدم الخدمة من الموقع الرسمي، أو من مركز التحميل الخاص بالتطبيقات للهواتف الذكية المعتمدة (App Store، Google Play وغيرها).
- تفعيل المصادقة الثنائية أو متعددة العوامل، كإرسال رمز تحقق لهاتف العميل.
- استخدام الأجهزة الحاسوبية ذات التحديث الأخير، وبوجود برامج الحماية المناسبة.
- التأكد من الاتصال الآمن للمواقع الإلكترونية بوجود رمز القفل في أعلى المتصفح.
- الاحتفاظ بالإيصالات الإلكترونية للعمليات المالية الرقمية.



- الأولوية أثناء الدفع المالي يكون باستخدام بطاقات الائتمان حيث -في أغلب الحالات- يتم إعادة المبلغ عند التعرض لعملية احتيال.
- استخدام وسائل الدفع الإلكترونية الآمنة مثل: (PayPal أو Apple Pay أو Google Pay) وغيرها من خدمات الدفع الآمن التي لا تعرض تفاصيل حساب العميل للغير (سيتم التطرق للإجراءات الآمنة بشكل عملي خلال دروس الوحدة الثالثة).

نشاط



طبق بعض إرشادات الحماية التي تعلمتها أعلاه على المعاملات المالية الرقمية التي تمارسها بشكل يومي، أو شارك الإرشادات مع بعض أفراد عائلتك، واكتب تقريراً بذلك.

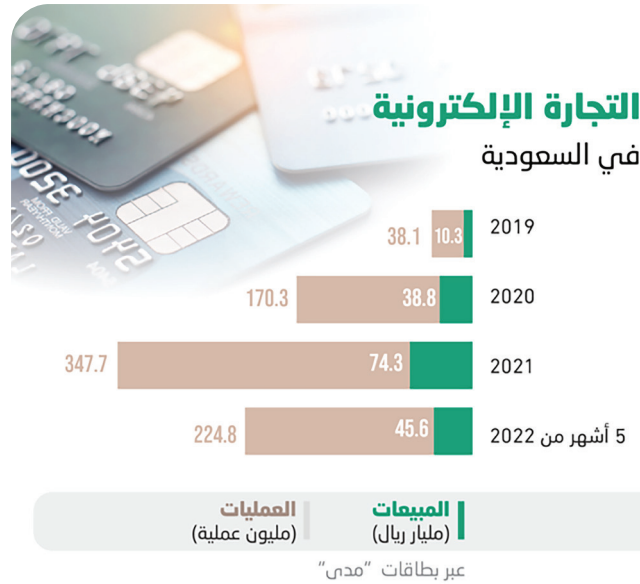
دور التجارة الإلكترونية في تحسين جودة الحياة

سهلت التجارة الإلكترونية كثيرًا من مجالات الحياة التي عانى منها الإنسان لسنوات عديدة مضت، وساهمت التجارة الإلكترونية في رفع اقتصاد الدول ونموها عبر دعمها من قبل الحكومات لدفع الاقتصاد إلى الأمام، وفتح الفرص للتجار للنمو والتوسع، ومن ثمّ ازدهار أعمالهم، وزيادة الوظائف، ويظهر الشكل (20-1) الدول الأكثر نموًا في مجال التجارة الإلكترونية.



شكل (20-1): حجم التجارة الإلكترونية لأكبر الأسواق في العالم-المصدر: Business.com

ودلت الإحصائيات إلى ازدياد نمو التجارة الإلكترونية في المملكة العربية السعودية بشكل ملحوظ خلال السنوات الأخيرة كما يظهر في الشكل (21-1):



شكل (21-1): إحصائيات التجارة الإلكترونية في السعودية من عام (2019 - 2022م) -المصدر: جريدة الاقتصادية

نمو التجارة الإلكترونية يؤدي إلى استحداث مجالات دخل عديدة للشركات والأفراد، وهي من أهداف برامج جودة الحياة ضمن رؤية المملكة العربية السعودية 2030 التي تدعو إلى تحسين جودة الحياة، وتوليد الوظائف، وتنويع النشاط الاقتصادي، وحجم الفوائد التي تعود على كل من المستهلك والتاجر كما في الجدول (1-1) الآتي:

جدول (1-1): فوائد التجارة الإلكترونية للمستهلك والتاجر

الفوائد التي تعود على المستهلك	الفوائد التي تعود على التاجر
تنوع في السلع والخدمات المحلية والعالمية.	التكلفة المنخفضة لتجهيز المتجر مقارنة بالموجود على أرض الواقع، وقلة المخاطر.
توفير الجهد والوقت أثناء عملية التسوق الرقمي.	التسويق المتعدد للمنتجات بأقل تكلفة وباستخدام تقنيات متطورة.
توفر السلع بأسعار تنافسية مقارنة بالواقع.	الوصول إلى كم كبير من المستهلكين، والاستفادة من بياناتهم، والتواصل معهم.
مقارنة السلع ببعضها لاختيار المناسب حسب معايير محددة من قبل المستهلك.	البيع الموسع في الداخل والخارج.
الاستفادة من خدمات الشحن العالمية.	التوسع السريع الذي يؤدي لزيادة الأرباح.

على المواطن الرقمي الاستفادة من هذه الفرص، وأن يكون واعياً وذكياً أثناء التعامل بالتجارة الإلكترونية سواء كان تاجرًا أو مستهلكًا، وأن يحافظ على أمواله خلال التسوق، وألا يشتري إلا ما يحتاج إليه، حفظاً لماله، وعدم الإسراف في الشراء عملاً بما ذكر في الحديث الشريف: (إِنَّ اللَّهَ كَرِهَ لَكُمْ ثَلَاثًا: قِيلَ وَقَالَ، وَإِضَاعَةَ الْمَالِ، وَكَثْرَةَ السُّؤَالِ) [رواه مسلم : 593]

التعامل مع المتاجر الإلكترونية بأمان

نشاط

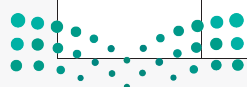


أثناء تجهيز الحفل العائلي السنوي، تم إسناد مهمة توفير مجموعة من الجوائز التكرمية للابن الشاب خالد بحيث توزع هذه الجوائز على الأبناء والبنات المتفوقين دراسياً، والخريجين من المرحلة الجامعية، وتتكون الجوائز من (عطور، ساعات، أقلام فاخرة)، وتم تحديد ميزانية مالية لشراء الجوائز تبلغ (10,000) ريال، وأشار أحد أقرباء خالد بشراء الجوائز من المتاجر الإلكترونية العالمية للحصول على أسعار منافسة تناسب الميزانية المحددة.

حلل أداء الابن خالد بين الاستخدام الملائم، وغير الملائم أثناء التسوق الإلكتروني من شبكة الإنترنت كما في الجدول

الآتي:

م	السيناريو	ملائم	غير ملائم
1	الشراء بقيمة أكثر من الميزانية المحددة والطلب من العائلة زيادة المبلغ.		
2	الشراء من متجر يعرض القيمة الأقل من بين المتاجر الأخرى.		
3	الشراء من متجر غير موثوق يعرض قيمة للمنتج أقل من متجر موثوق يقدم قيمة أعلى.		
4	الشراء من أول متجر يعثر عليه خالد.		
5	الاستفسار من الأقرباء أو الزملاء عن أفضل المتاجر الموثوقة والأمنة.		
6	استهلاك بعض الوقت في البحث بين المتاجر لانتقاء الأنسب منها		
7	معرفة الوقت المحدد لوصول البضاعة إلى المدينة التي يسكن بها		
8	التسجيل في حساب العميل في المتجر مباشرة قبل البحث عن توفر المنتجات المناسبة.		



يلاحظ من الجدول السابق، مجموعة من الممارسات التي ينصح المواطن الرقمي اتباعها لإجراء عملية تسوق إلكترونية، وفيما يأتي أهم النصائح أثناء التعامل مع المتاجر الإلكترونية المحلية والعالمية لبدء تسوق آمن عبر الإنترنت (Safe Online Shopping):

- الشراء من المواقع المعروفة التي سبق تجربتها من قبل الآخرين، فهناك عددٌ من المتاجر التي تقدم عروضاً وخصومات تكون غطاء لمواقع انتحال.
- استخدام بطاقة شرائية (مسبقة الدفع)، ويتم تغذيتها بشكل دوري وفق الحاجة، وعدم حفظها في المتجر بعد إتمام عملية الشراء.
- التقليل من مشاركة معلوماتك الشخصية مع المتاجر، وكن حذراً من المواقع التي تطلب بيانات ليس لها علاقة بالشراء.
- استخدام كلمات مرور مختلفة لحسابات المتاجر، والحرص على أن تكون صعبة التخمين.
- الحرص على التأكد من وجود المتجر السعودي ضمن قائمة المتاجر المصنفة والموثوقة في "منصة الأعمال" التابعة للمركز السعودي للأعمال.
- عدم الشراء من أجهزة الحاسب العامة، أو المتصلة بشبكة الواي- فاي المفتوحة.
- قلل المعلومات التي تضعها في المتجر عند إجراء عملية الشراء قدر الإمكان.
- لا تفتح حساباً لدى المتجر إذا كان بالإمكان الشراء بحسابات الدفع الإلكترونية الآمنة.

تواصل مباشرة مع البنك التابع لبطاقتك لإيقافها عند تعرضك لأي عملية احتيالية، وقدم بلاغ جريمة معلوماتية عن الجهة التي تعرضت للاحتيال منها.



|| كن مستهلكاً ذكياً

لتكون متسوقاً ذكياً عليك اتباع مجموعة من الخطوات العامة المرتبة التي يمكن إيجازها في الشكل (1-22):

أولاً اختر بعناية المتجر الإلكتروني الذي تتسوق منه.

ثانياً اعرف كافة معلومات عن السلعة المراد شراءها.

ثالثاً اقرأ مراجعات المنتج من قبل العملاء الآخرين.



رابعاً

تعرف على كيفية قراءة شروط وأحكام المشتريات.

خامساً

تعرف على آلية إضافة الرسوم الإضافية على المنتجات كالضريبة المحلية ورسوم الجمارك ورسوم الشحن.

سادساً

تعرف على آلية إرجاع المنتج إلى المصدر بعد استلامه لأي أسباب مصنعية.

سابعاً

قارن بين المنتجات في أكثر من متجر، واستفد من المواقع التي تقدم هذه الخدمة، للاستفادة من الأسعار الأقل، والضمان الأفضل، وتمييز نوع للمنتج (أصلي، غير أصلي) مع المنتج في الشركة المصنعة.

ثامناً

ضع تعليق على المنتج أو الخدمة إذا كانت دون المستوى.

شكل (22-1): خطوات الاستهلاك الذكي

نشاط



تأمل وناقش) لماذا يجب على المواطن الرقمي أن يكون مستهلكاً ذكياً أثناء التسوق من شبكة الإنترنت؟

إثراء



يوجد العديد من مواقع المزادات المحلية والعالمية التي يستطيع الفرد الدخول والقيام بعملية المزايدة والشراء والبيع من خلالها، ويجب على المتسوق البحث بشكل متعمق عن مصداقية هذه المواقع، وكيفية التعامل معها. يوفر موقع (كن آمناً عبر شبكة الإنترنت) مجموعة من النصائح عند المشاركة لهذه المزادات لاستعراض هذه النصائح، امسح رمز الاستجابة السريع.

من خلال ما سبق، استنتج خمسة من أبرز الفوائد والمكاسب التي يمكنك بها إقناع الفرد للتحول من مستهلك عادي إلى مستهلك ذكي أثناء التسوق لاحتياجاته اليومية أو الموسمية.

-
-
-
-
-

خطوات إنشاء متجر إلكتروني (Online Store):

أصبحت المتاجر الإلكترونية في العصر الحالي من المصادر الرئيسية للمستهلك التي يمكنه الاعتماد عليها في التسوق، وشراء الخدمات الإلكترونية، والوصول إلى العميل في موقعه السكني، وزيادة التوسع والنمو والكسب المادي أكثر من التجارة التقليدية.



المتجر الإلكتروني عبارة عن منصة إلكترونية يمكن من خلالها بيع المنتجات الملموسة كاللبضائع المادية التي نلمسها باليد، والمنتجات غير الملموسة كالخدمات الإلكترونية المتعددة كالتصميم والمونتاج وبناء المواقع والبرمجيات، وكل ما له صفة رقمية. تدار عملية الشراء والبيع بنظام الأتمتة المتكاملة (بشكل آلي) بدون تدخل الإنسان، ويوفر المتجر الإلكتروني الموصفات الكاملة للمنتج من نصوص وصور ومقاطع مرئية، وكذلك طرق الدفع والاسترجاع، ومدة الضمان، وبيانات الشحن إلى المنزل.



ربما يهملك قبل الدخول في التجارة الإلكترونية معرفة بعض المكاسب والأرباح التي حققها أصحاب المتاجر العالمية المشهورة في قطاع التجزئة مثل:

- Amazon.com: موقع عالمي حقق ما يقرب من 121 مليار دولار.
- JD.com: موقع صيني حقق أكثر من 83 مليار دولار.
- Walmart.com: موقع أمريكي حقق 41.1 مليار دولار.
- Apple.com: موقع أمريكي في مجال التقنية حقق 32 مليار دولار.
- Suning.com: موقع صيني في مجال الملابس حقق 21 مليار دولار (المصدر: 2023 - www.business.com).



وللدخول في عالم التجارة الإلكترونية، يمكن البدء في بناء متجر إلكتروني باتباع الخطوات الآتية:

الخطوة الأولى

- الاطلاع على القوانين والقواعد المنظمة لممارسة التجارة الإلكترونية وأخذ فكرة واسعة قبل البدء في المشروع

الخطوة الثانية

- تحديد المنتج المراد بيعه، ويعتمد على كون صاحب المتجر هو المالك الوحيد والمصنّع للمنتج، أو تقديم منتجات تقليدية متوفرة في السوق، ويراعى في اختيار المنتج ما يلي:
- تحديد فئة المنتج.
- تحديد نوع المنتج.
- قابلية بيع المنتج عبر الإنترنت.
- البحث عن المنتجات التي تلبي رغبة العملاء، وذات العلامة التجارية المحتملة.

الخطوة الثالثة

- عمل دراسة على المنتج المختار، وعمل بحث موسع عن مبيعاته في المتاجر العالمية المعروفة.

الخطوة الرابعة

- تحديد اسم المتجر ويكون فريداً من نوعه، ومن ثم حجز المتجر الإلكتروني عبر الحجز عند أحد مقدمي المتاجر الإلكترونية المحلية أو العالمية (مقابل رسم مالي أو مجاني).

الخطوة الخامسة

- إصدار التصاريح المناسبة (فتح سجل تجاري) أو (إصدار وثيقة عمل حر).
- توثيق المتجر في (منصة الأعمال) ليكون المتجر أكثر ثقة للعملاء.

الخطوة السادسة

- تحديد وسائل الدفع الإلكترونية المناسبة، وطرق الشحن المعتمدة.

الخطوة السابعة

- عمل خطة تسويق مناسبة للمتجر الإلكتروني.



شكل (23-1): خطوات بناء متجر إلكتروني

الجهود المبذولة من المملكة العربية السعودية لتوفير تجارة رقمية آمنة.

أولت حكومة المملكة العربية السعودية عبر محور رؤية 2030 "الاقتصاد المزدهر" جانب من اهتمامها بقطاع التجارة الإلكترونية بتشريع نظام التجارة الإلكترونية، وسنّ الأنظمة واللوائح، وتطوير البنية التحتية الرقمية وإنشاء المنصات الإلكترونية الحكومية لإنجاز الأعمال بكفاءة، ودعم الصادرات السعودية عبر منصات التجارة الإلكترونية، ودعم المنشآت الصغيرة والمتوسطة، وهذا ما يدفع بدوره عجلة الاقتصاد الرقمي إلى الأمام. يمكن إيجاز بعض الجهود الرئيسة التي قدمتها المملكة في دعم التجارة الإلكترونية فيما يأتي:

تأسس مجلس التجارة الإلكترونية في 5 ذو القعدة 1439هـ، ليكون منطلقاً للجهود المتكاملة لجميع الجهات الوطنية ذات العلاقة، ويسهم في اقتراح سياسات التجارة الإلكترونية، وتشريعاتها، والتنسيق لمنع العوائق التي تواجه التجارة الإلكترونية، وضمان التنفيذ الفاعل للمشاريع، وتحفيز التجارة الإلكترونية.



وفرت وزارة التجارة مجموعة من الأدلة والإرشادات للدخول في عالم التجارة الإلكترونية عبر موقعها في شبكة الإنترنت، التي تنظم عمل المواطن، وأخذ التصاريح اللازمة لذلك، وللوصول إلى الصفحة امسح رمز الاستجابة السريع.



تبنت الهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت" تقديم حزمة من الخدمات التي تمكّن رواد الأعمال من الاستفادة من الفرص والالتحاق بالتجارة الإلكترونية وبناء متاجر خاصة بهم، وتقديم الدعم الاستشاري والمادي، وللوصول إلى الصفحة امسح رمز الاستجابة السريع.



- كيف تحولت بعض المتاجر الصغيرة إلى متاجر عالمية معروفة وبعضها لم تحقق ذلك؟
- ما الصفات التي يجب أن يمتلكها المتجر الإلكتروني حتى يصل إلى مصاف المتاجر العالمية؟

نقاط مهمة

- عند فتح متجر إلكتروني، يمكنك إنشاء حساب بنكي مخصص باسم المتجر لتكون المعاملات المالية مباشرة باسمه.
- يشترط لاستخراج وثيقة عمل حر وجود ما يثبت للمتقدم بحصوله على شهادات تدريبية أو خبرة سابقة في مجال النشاط المقدم عليه.
- مشوار الألف ميل يبدأ بخطوة، فنجاح مشروع متجر إلكتروني يحتاج مزيداً من الصبر، والتخطيط السليم، ودراسة الواقع بعناية.
- قد لا تكون الأسعار دائماً في المتاجر الإلكترونية الأفضل على الإطلاق، تتبع دائماً مواسم التخفيضات المحلية، وكن مستعداً لذلك.



مشروع الدرس



الموضوع: اختر أحد موضوعي الدرس الآتيين:

- التعاملات المالية الرقمية.
- التسوق الآمن عبر شبكة الإنترنت.

الهدف: توعية مجتمعية.

طريقة التنفيذ: تصميم رسم معلوماتي (Infographic)، إنتاج مقطع مرئي (Video).

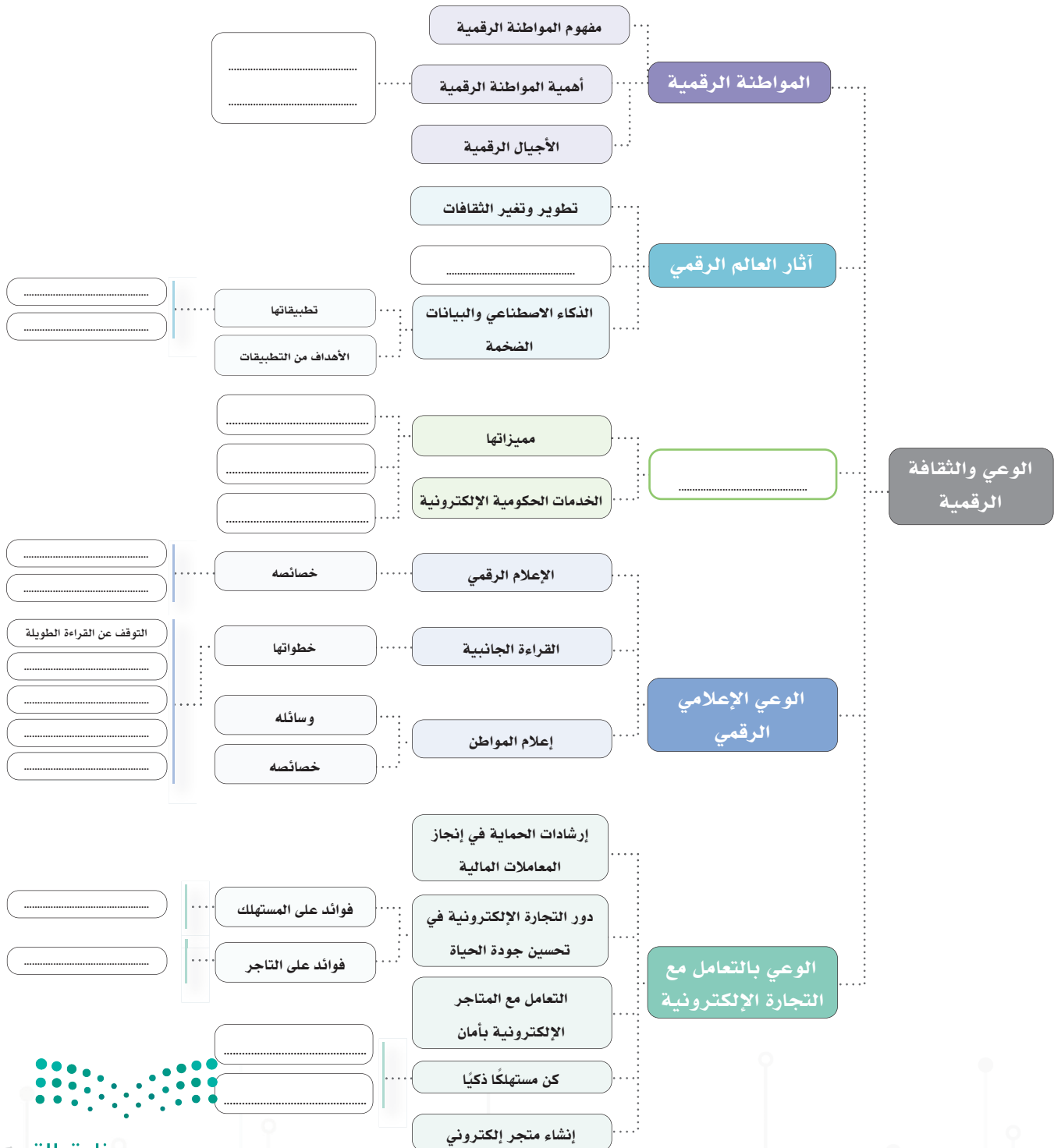
طريقة التقديم:

- النشر في مدونة الطالب الشخصية.
- النشر في إحدى وسائل التواصل الاجتماعي.



خارطة مفاهيم الوحدة

أكمل الخارطة المفاهيمية الآتية:



تقويم الوحدة

السؤال الأول: ضع إشارة (✓) أمام العبارة الصحيحة وإشارة (X) أمام العبارة الخطأ:

العبارة	الإجابة
1. تركز المواطنة الرقمية على إعداد مجتمع لاستخدام التقنيات الرقمية بكفاءة وفعالية.	
2. تعكس المواطنة الرقمية هوية الفرد الإسلامية في الحياة الواقعية.	
3. جيل المهاجر الرقمي وُلد في وجود التقنية الرقمية.	
4. تم تحويل 80% من الخدمات الحكومية لتكون رقمية.	
5. تعدُّ الدعاية المكتسبة من تفاعل الجمهور أحد قنوات الإعلام المدفوعة.	
6. يعمل المتجر الإلكتروني على بيع المنتجات المادية فقط عند طلبها من العميل.	
7. العالم الرقمي أثر بشكل واضح على تغيّر الثقافات في المجتمعات.	
8. يمكن التحقق من الأحقية في الحج عبر منصة أبشر.	
9. الهدف من الدورات التدريبية الحصول على الشهادة التدريبية والاكتفاء بذلك.	
10. ليس دوري كمواطن رقمي أن أبرز صورة هويتي الإسلامية.	
11. خدمة "أمر" مخصصة للرد على استفسارات المواطنين والمقيمين ومساعدتهم في الاستفادة من الخدمات الحكومية الإلكترونية.	
12. أول ما يتم عمله عند التسوق عبر الإنترنت هو اختيار المتجر بعناية.	
13. المعلومات الزائفة هي معلومات غير صحيحة يتم نشرها عمدًا بهدف تضليل الجمهور أو توجيههم.	
14. تهتم القراءة الجانبية بتقييم مصداقية المادة الإعلامية من خلال مقارنتها بمصادر أخرى.	
15. لا نحتاج أنظمة الذكاء الاصطناعي إلى أي بيانات، وإنما تستطيع توليد البيانات من تلقاء نفسها.	



السؤال الثاني: اختر الإجابة الصحيحة في كل مما يأتي:

الجملة	الخيارات
1. المفهوم الذي يدل على إعداد المواطن ليكون مسؤولاً عن تصرفاته في العالم الرقمي:	أ. المواطنة الرقمية.
	ب. المواطنة العالمية.
	ج. المواطنة الصالحة.
2. من تداعيات العالم الرقمي على المجتمعات:	أ. التقارب بين الثقافات.
	ب. التباعد بين الثقافات.
	ج. التنافر بين الثقافات.
3. من مميزات الخدمات الرقمية أنها:	أ. تزيد من رضا المستفيدين.
	ب. تحتكر البيانات.
	ج. تخدم المواطنين والمقيمين فقط.
4. دور المواطن المسلم تجاه العالم الرقمي هو المحافظة على ثقافته وهويته الإسلامية عبر:	أ. انعزاله عن الدخول إلى العالم الرقمي.
	ب. فصله بين الهوية الإسلامية والعالم الرقمي.
	ج. إبرازه لصورة الإسلام.
5. من خصائص الإعلام الرقمي:	أ. يقوم به المتخصص في الإعلام.
	ب. موثوقية المعلومات.
	ج. سرعة الانتشار.



الجملة	الخيارات
6. للتحقق من صحة المادة الإعلامية يمكن البحث في:	أ. الصحف التجارية الإلكترونية. ب. الرجوع لمصدر الخبر الأصلي. ج. وسائل التواصل الاجتماعي.
7. يعود النمو والتوسع في التجارة الإلكترونية على الدول إلى:	أ. رفع اقتصادها. ب. تحجيم النشاط المحلي. ج. تقليل عدد الوظائف.
8. من النصائح المهمة عند بدء التسوق عبر المتاجر الإلكترونية:	أ. طريقة الدفع المتاحة. ب. البحث عن المتجر الموثوق. ج. البحث عن أصناف للمنتج.
9. من أمثلة محظورات النشر حسب نظام المطبوعات والنشر في المملكة العربية السعودية:	أ. كتابة تعليق ينتقد الخدمة في أحد المطاعم. ب. نشر صور ومقاطع من الحياة الشخصية. ج. نشر مقطع صوتي سيء لمفتي المملكة العربية السعودية.

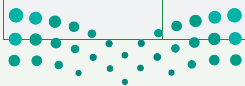


أقيّم ما تعلّمت في الوحدة

بناءً على ما تعلّمت من دروس في هذه الوحدة؛ قيّم نفسك ذاتياً عبر معايير التقييم الموضحة في الجدول، واحسب مجموع النقاط المكتسبة.

- 2 = ينطبق بدرجة عالية.
- 1 = ينطبق بدرجة متوسطة.
- 0 = لا ينطبق.

النقاط المكتسبة	مقاييس التقييم			مقياس التقييم
	0	1	2	
2/.....	لم اقترح مفهوم للمواطنة الرقمية، ولم أستنتج أي من عناصرها.	اقترحت مفهوم للمواطنة الرقمية بشكل مقبول، واستنتجت ثلاثة من عناصرها.	اقترحت مفهوم للمواطنة الرقمية بشكل صحيح، واستنتجت ستة من عناصرها.	1. تعريف مفهوم المواطنة الرقمية، واستنتاج عناصرها.
2/.....	لم أعدد أي محور للمواطنة الرقمية في المقرر.	عددت اثنين من محاور المواطنة الرقمية في المقرر.	عددت ثلاثة من محاور المواطنة الرقمية في المقرر.	2. تعداد محاور المواطنة الرقمية.
2/.....	لم أذكر أي أمثلة على تأثير العالم الرقمي في تغيير الثقافات.	ذكرت أربعة أمثلة على تأثير العالم الرقمي في تغيير الثقافات.	ذكرت ستة أمثلة على تأثير العالم الرقمي في تغيير الثقافات.	3. ذكر أمثلة على تأثير العالم الرقمي في تغيير الثقافات.
2/.....	لم التحق بأي دورة تدريبية.	التحقت بدورة تدريبية واحدة ولم أنهي الدروة.	أتممت دورة تدريبية واحدة في إحدى منصات التدريب.	4. الالتحاق بدورة تدريبية لتطوير كفاياتي المهنية.
2/.....	لم أبحث عن أي من مهن للمستقبل.	بحثت وتوصلت إلى خمسة مهن للمستقبل.	بحثت وتوصلت إلى عشرة مهن للمستقبل.	5. البحث عن مهن المستقبل عبر شبكة الإنترنت.
2/.....	لم أعرف مفهوم الخدمات الرقمية، ولم أعدد أي من مميزاتها.	عرفت مفهوم الخدمات الرقمية بشكل مقبول، وعددت 4 من مميزاتها.	عرفت مفهوم الخدمات الرقمية بشكل صحيح، وعددت 8 من مميزاتها.	6. أتعرف على مفهوم الخدمات الرقمية وأهم مميزاتها.
2/.....	لم اقترح أي تطبيق رقمي.	اقترحت تطبيقين رقميين خدمية.	اقترحت ثلاثة تطبيقات رقمية خدمية.	7. اقتراح تطبيقات لخدمات رقمية حكومية تسهم في خدمة المجتمع.



أقيّم ما تعلّمت في الوحدة

النقاط المكتسبة	مقاييس التقدير			معيّار التقييم
	0	1	2	
2/.....	لم استخدم تطبيق أبشر على الإطلاق	استخدمت تطبيق أبشر واستعلمت عن خدمة واحدة من الخدمات الرقمية.	استخدمت تطبيق أبشر، واستعلمت عن اثنين على الأقل من الخدمات الرقمية.	8. استخدام تطبيق أبشر الحكومي.
2/.....	لم أعرف مفهوم الوعي الإعلامي الرقمي، ولم أعد أي من أبعاده.	عرفت مفهوم الوعي الإعلامي الرقمي بشكل مقبول، وعددت اثنين من أبعاده.	عرفت مفهوم الوعي الإعلامي الرقمي بشكل صحيح، وعددت أبعاده الثلاثة.	9. تعريف مفهوم الوعي الإعلامي الرقمي وتعداد أبعاده.
2/.....	لم أعد أي من خصائص الإعلام الرقمي، أو أعد أي من قنواته.	عددت ثلاث من خصائص الإعلام الرقمي، وعددت اثنين من قنواته.	عددت ست من خصائص الإعلام الرقمي، وعددت أربعة من قنواته.	10. تعداد خصائص الإعلام الرقمي، وتعداد قنواته.
2/.....	لم أعرف مهارة القراءة الجانبية، ولم أعد أي من خطواتها.	عرفت مهارة القراءة الجانبية بشكل مقبول، وعددت ثلاثاً من خطواتها.	عرفت مهارة القراءة الجانبية بشكل صحيح، وعددت خطواتها الخمسة.	11. تعريف مهارة القراءة الجانبية، وتعداد خطواتها.
2/.....	لم أعرف مفهوم إعلام المواطن، ولم أعد أي من وسائله أو خصائصه.	عرفت مفهوم إعلام المواطن بشكل مقبول، وعددت ثلاثة من وسائله، وثلاثاً من خصائصه.	عرفت مفهوم إعلام المواطن بشكل صحيح، وعددت وسائله الخمسة، وخصائصه الخمسة.	12. تعريف مفهوم إعلام المواطن، ووسائله، وخصائصه.
2/.....	لم أعرف مفهوم التجارة الإلكترونية.	عرفت مفهوم التجارة الإلكترونية بشكل مقبول.	عرفت مفهوم التجارة الإلكترونية بشكل صحيح.	13. تعريف مفهوم التجارة الإلكترونية.
2/.....	لم أعد إرشادات الحماية لإنجاز المعاملات المالية الرقمية.	عددت من (1) إلى (4) إرشادات لإنجاز المعاملات الرقمية المالية.	عددت من (5) إلى (8) إرشادات لإنجاز المعاملات الرقمية المالية.	14. تعداد إرشادات الحماية لإنجاز المعاملات الرقمية المالية.
2/.....	لم أعد نصائح التسوق الآمن من المتاجر الإلكترونية	عددت من (1) إلى (4) نصائح للتسوق الآمن من المتاجر الإلكترونية	عددت من (5) إلى (8) نصائح للتسوق الآمن من المتاجر الإلكترونية.	15. تعداد النصائح الآمنة للتسوق من المتاجر الإلكترونية.
30/.....	المجموع			

لحساب مجموع النقاط:

- 20 فأعلى = متمكن بدرجة عالية.
- من 14 إلى 19 = متمكن إلى حدٍ ما.
- أقل من 14 = غير متمكن.





الوحدة الثانية



وزارة التعليم

Ministry of Education

2023 - 1445

الاحترام والمسؤولية الرقمية

Digital Respect and Responsibility

تهدف هذه الوحدة إلى تمكين المواطن الرقمي من إدارة حضوره الرقمي بوعي ومسؤولية بشكل يعكس هويته الإسلامية والوطنية، وتزويده بالمعارف، والمهارات، والقيم التي تساعد على بناء بصمة وسمعة رقمية إيجابية، والوعي بأنواع العلاقات الرقمية، وكيفية إدارتها بشكل فعال، إضافة إلى الانتباه لأشكال العنف الرقمي، وكيفية التعامل معها، والتمكّن للوصول إلى حالة الاتزان الرقمي.

متطلبات الوحدة

تحتوي بعض الدروس على تطبيقات عملية تحتاج إلى توفير جهاز حاسوب، خدمة إنترنت، برامج تصميم، تطبيقات الهواتف الذكية.



أهداف التعلم

1. تعريف مفهوم الهوية الرقمية، والبصمة الرقمية، والسمعة الرقمية ودورها في تعزيز الحضور الإيجابي عبر الإنترنت.
2. تطبيق مهارات إدارة البصمة الرقمية والسمعة الرقمية.
3. استشعار أهمية بناء هوية وسمعة رقمية إيجابية وأثر ذلك على القبول في الجامعات والوظائف مستقبلاً.
4. ممارسة الآداب والأخلاقيات للمواطنة الرقمية الصالحة.
5. تقدير أهمية قيمة التعاطف في توجيه السلوك المسؤول في العالم الرقمي.
6. تمييز العلاقات الرقمية الصحية وغير الصحية والعلاقات الرقمية الخطرة.
7. وضع حدود صحية للعلاقات الرقمية.
8. المشاركة في حوار متحضر عبر شبكة الإنترنت.
9. تمييز أشكال العنف الإلكتروني والطرق الفعالة للتعامل معها.
10. تثمين جهود المملكة لمكافحة أشكال العنف الإلكتروني.
11. استشعار دور القيم في الحد من ظاهرة العنف الإلكتروني.
12. المشاركة في التوعية بأشكال العنف الإلكتروني وأسبابها وطرق الحد منها.
13. شرح المخاطر الصحية والاجتماعية المرتبطة بالإدمان الرقمي.
14. استخدام التطبيقات الرقمية لتحسين الصحة.
15. تطبيق الطرق المساعدة في الوصول للاتزان الرقمي.
16. المساهمة في التوعية المجتمعية بأخطار الإدمان الرقمي، وسبل تحقيق الاتزان الرقمي.





الهوية الرقمية

مخرجات التعلم:

- أتعرف على مفهوم الهوية الرقمية.
- أميز بين أنواع الهويات في العالم الرقمي.
- أستنتج دور وسائل التواصل الاجتماعي في التأثير على الأفراد لبناء الهوية الرقمية.
- أتعرف على مفهوم البصمة الرقمية وخصائصها.
- أتعرف على مفهوم السمعة الرقمية ووسائل حمايتها.
- أفرق بين مفاهيم الهوية الرقمية والبصمة الرقمية والسمعة الرقمية.
- أناقش أهمية البصمة الرقمية والسمعة الرقمية ودورها في التأثير على مستقبلي.
- أدير بصمتي وسمعتي الرقمية بمهارة.
- أساهم في التوعية المجتمعية بكيفية بناء هوية رقمية إيجابية.



مصطلحات الدرس:

- الهوية الرقمية (Digital Identity)
- البصمة الرقمية (Digital Footprint)
- السمعة الرقمية (Digital Reputation)

التهيئة

في ظل التنامي المتزايد لاستخدام شبكة الإنترنت ووسائل التواصل الاجتماعي ظهر ما يسمى بالهوية الرقمية كوسيلة يستخدمها الأفراد للتواصل وإثبات تواجدهم الرقمي، وهذه الهوية قد تكون مشابهة أو مخالفة لهوية الشخص في العالم الواقعي، وظهرت أيضاً مفاهيم أخرى ذات علاقة بالهوية وهي البصمة الرقمية والسمعة الرقمية، ومن هذا المنطلق يمكن التساؤل:

- كيف أثرت وسائل التواصل الاجتماعي في بناء الهوية الرقمية للأفراد؟
- إلى أي مدى تعكس الهوية الرقمية للأفراد هويتهم الحقيقية؟
- كيف يمكن أن تؤثر بصمتنا الرقمية على حاضرتنا ومستقبلنا؟
- هل يوجد من يستهدف بصمتنا الرقمية؟ كيف؟ ولماذا؟
- كيف يمكن أن يؤثر ما ينشره الوالدان على هوية وسمعة أبنائهم في المستقبل؟
- وفي المقابل، كيف يمكن أن يؤثر ما ينشره الأبناء عن والديهم على سمعتهم ومكانتهم الاجتماعية؟

الهوية الرقمية

الهوية الرقمية (Digital Identity) هي الهوية التي يبنها مستخدم الإنترنت بهدف التواجد والتواصل في المجتمعات الرقمية، ويوجد ثلاثة عوامل رئيسة تُشكل الهوية الرقمية:

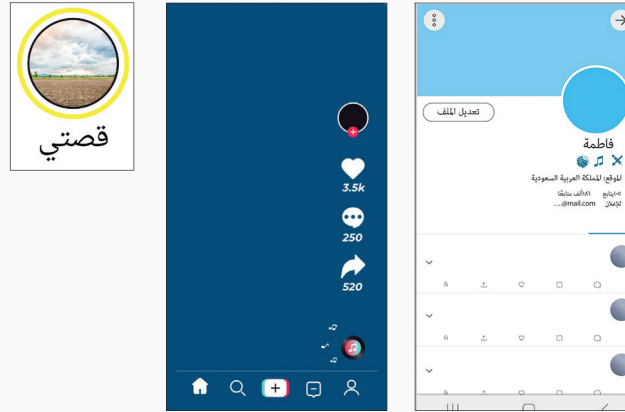
1. المعلومات الشخصية: المعلومات التعريفية التي تدل على شخصية المستخدم مثل: الاسم، الصورة التعريفية، الموقع الجغرافي (لأي دولة ينتمي)، معلومات عن مكان العمل، المؤلفات والمنشورات، الهوايات، الحالة الاجتماعية وغيرها من المعلومات الشخصية التي يتم مشاركتها عبر الملف التعريفي.
2. النشاط في العالم الرقمي: كل نشاط يقوم به المستخدم عبر شبكة الإنترنت، ويشمل ذلك تاريخ البحث في شبكة الإنترنت، المنشورات في وسائل التواصل الاجتماعي والمنصات الرقمية المختلفة، الألعاب والمعاملات عبر شبكة الإنترنت.
3. التغذية الراجعة من الآخر (المتابعين): ردة الفعل والتفاعل الذي يحصل عليه المستخدم من المتابعين، عبر الإعجاب والتعليقات وإعادة مشاركة المنشورات.

نشاط



1-2

حلل الصور الظاهرة في الشكل (1-2)، واستنتج منها كيف يتم بناء الهوية الرقمية؟



شكل (1-2): عوامل بناء الهوية الرقمية

من العوامل المساعدة في بناء الهوية الرقمية:

1.

2.

3.

4.



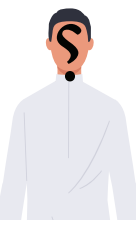
أشكال الهوية الرقمية

يوضح الشكل (2-2) أشكال الهوية الرقمية حيث يختلف شكل الهوية لدى مستخدمي شبكة الإنترنت ووسائل التواصل الاجتماعي في العالم الرقمي، ومنها:



الهوية المأمولة

وهي الهوية التي يمزج فيها المستخدم بين معلومات حقيقية وأخرى مزيفة، حيث يظهر المستخدم نفسه بشكل مبالغ فيه مخالفاً للواقع مثل ادعاء امتلاك شهادات أو مناصب أو خبرات معينة.



الهوية المجهولة أو المزيفة

وهي التي يظهر المستخدم من خلالها باسم رمزي ومعلومات مزيفة، ويحرص على عدم التعريف بهويته الحقيقية.



الهوية الحقيقية

وهي التي يظهر فيها المستخدم بمعلومات صحيحة عن نفسه، من اسمه، ومستواه التعليمي ونشاطاته واهتماماته.

شكل (2-2): أشكال الهوية الرقمية

نشاط



مقياس الهوية الرقمية:

باستخدام المقياس الآتي تأمل إلى أي مدى تتشابه هويتك الرقمية مع هويتك الحقيقية.

قيم هويتك الرقمية باستخدام المعايير في الجدول الآتي، حيث إن:

(2) ينطبق - (1) ينطبق إلى حد ما - (0) لا ينطبق.

ملاحظة: إذا كان المجموع أقل من (6) فهذه إشارة إلى أن هويتك الرقمية لا تتشابه هويتك الحقيقية.

م	المعيار	التقييم
1	أستخدم اسمي الحقيقي في وسائل التواصل الاجتماعي.	
2	أستخدم صورتي الحقيقية في وسائل التواصل الاجتماعي.	
3	منشوراتي تعبر عن اهتماماتي وهواياتي.	
4	منشوراتي تعكس هويتي الإسلامية والوطنية.	
5	أوضح السبب لتواجدي الرقمي (تعليم، ترفيه، تواصل، مشاركة معلومات ...).	
6	شخصيتي في العالم الرقمي مشابهة لشخصيتي في العالم الواقعي.	
المجموع		



إثارة التفكير:

من واقع خبرتك، ما هي الأسباب التي تدفع مستخدمو وسائل التواصل الاجتماعي لتبني هوية مجهولة أو مأمولة؟

دور وسائل التواصل الاجتماعي في التأثير على الأفراد في بناء الهوية الرقمية

- لا شك أن لوسائل التواصل الاجتماعي وما تبثه من أفكار وصور نمطية عن الجمال والنجاح والتميز والسعادة وغيرها من الموضوعات أثر في تشكيل الأفراد لهويتهم في العالم الرقمي والواقعي. من الوسائل المستخدمة للتأثير على الأفراد:
- استخدام الإعلانات المدفوعة والتي تظهر للمستخدمين أثناء تصفحهم شبكة الإنترنت ومختلف وسائل التواصل الاجتماعي.
- الاستعانة بالمؤثرين في وسائل التواصل الاجتماعي للترويج للأفكار والاهتمامات والمنتجات المختلفة (صحة، جمال، سفر وسياحه وغيره من المنتجات).
- استخدام الخوارزميات والذكاء الاصطناعي وملفات الارتباط (cookies) حيث تساعد على تخصيص تجربة المستخدم من خلال تتبع نشاطه واستهدافه بالموضوعات والإعلانات.

نشاط



3-2

اقرأ النص الآتي واستنتج بعض الطرائق التي تستخدمها وسائل التواصل الاجتماعي والتي قد تؤثر على الأفراد في بناء هويتهم الرقمية.

بينما كان ياسر يتصفح حسابه في تويتر رأى تغريدة لأحد المؤثرين عن السفر للخارج، نقر ياسر زر الإعجاب لتفضيل هذه التغريدة، والعودة إليها في وقت لاحق، ثم انتقل ياسر لتصفح تطبيق التيك توك والذي بدأ بإظهار العديد من الإعلانات الخاصة بوكالات السفر والسياحة. بعد ذلك، نشر ياسر عبر صفحته على الانستغرام مجموعة من الصور والمقاطع الخاصة به عن رحلة سابقة.

استنتاجك:



مفهوم البصمة الرقمية



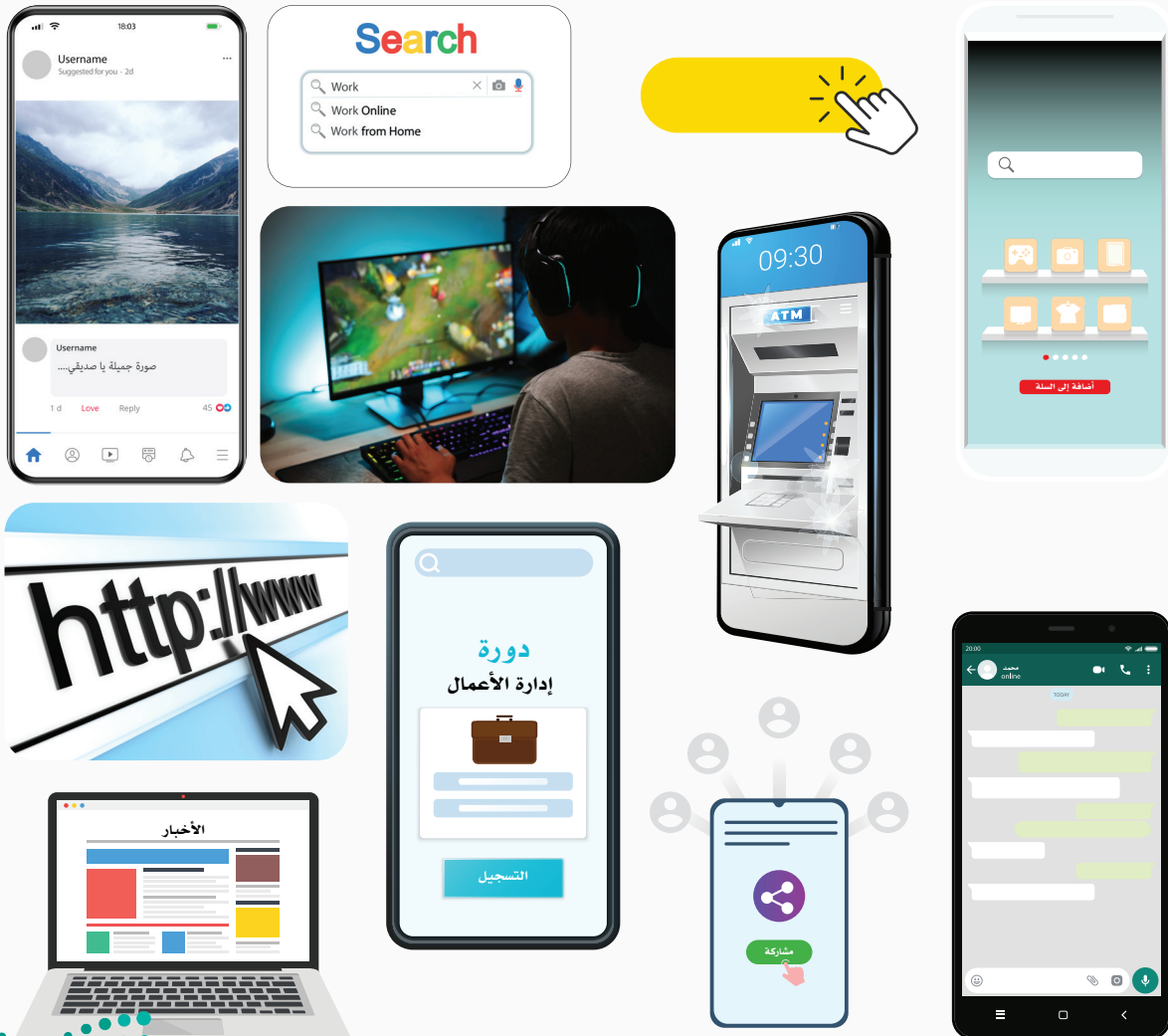
يقصد بالبصمة الرقمية (Digital Footprint) أثر البيانات والمعلومات التي يتركها الشخص عند استخدام شبكة الإنترنت عبر أنشطته الرقمية المختلفة، وهذه المعلومات قد يكون تم نشرها بواسطة الشخص نفسه أو بواسطة آخرين، عن قصد أو من غير قصد.

نشاط



4-2

اختر من الصور الظاهرة في الشكل (3-2) ما يمكن أن يشكل البصمة الرقمية لمستخدمي الإنترنت:



شكل (3-2): بعض أشكال الأنشطة الرقمية التي تشكل البصمة الرقمية



تشمل البصمة الرقمية البيانات الوصفية الخاصة بالمستخدم (metadata) وهي بيانات رقمية تصف خصائص المصادر الرقمية المتاحة على شبكة الإنترنت مثل: عنوان بروتوكول الإنترنت IP الخاص بجهاز المستخدم، الموقع الجغرافي الذي تم الإرسال منه، مدة المحادثات التي يقوم بها المستخدم، وهوية الشخص الذي يتم الاتصال به، وغيرها من البيانات.

خصائص البصمة الرقمية

1. يمكن للبصمة الرقمية أن تكشف الكثير عن مستخدمي شبكة الإنترنت واهتماماتهم وتوجهاتهم.
2. البيانات التي تبني منها البصمة الرقمية هي بيانات دائمة نسيًا حيث إنه لا يمكن إزالة الآثار الرقمية الناتجة عن الاستخدام حتى بعد الحذف.
3. سرعة مشاركة الملفات والتعليقات وتناقلها يجعل البصمة الرقمية للشخص تنتشر على نطاق واسع عبر شبكة الإنترنت، فبمجرد أن يتم النشر سواء على نطاق عام أو خاص لا يمكن للشخص المالك للمنشور السيطرة على كيفية استخدام الشخص الآخر لما تم نشره.
4. تؤثر البصمة الرقمية على مستقبل الأفراد سواء في مجال التوظيف أو القبول في الجامعات.
5. يمكن لمجرمي الإنترنت استغلال البصمة الرقمية للمستخدمين، مما قد يعرضهم للسرقة أو الابتزاز أو غيرها من الجرائم السيبرانية.



الجمهور الذي يمكنه الاطلاع على بصمتك الرقمية غير ظاهر لك كما في العالم الواقعي، فقد يكون هذا الجمهور عبارة عن أشخاص معروفين بالنسبة إليك -أقارب وأصدقاء- أو مجهولين وغير متوقعين يمكنهم رؤية معلومات عنك، كما يمكنهم حفظها ونشرها في الحال أو في وقت لاحق عبر الإنترنت.

نشاط



5-2

بعد معرفة أن كل نشاط تقوم به في العالم الرقمي يمكن تتبعه وتخزينه ونشره على نطاق واسع، كيف سينعكس ذلك على تواجدك الرقمي؟



اقرأ السيناريو الآتي:

ستقام فعالية في مدرستك عن «اليوم العالمي للصحة النفسية» وسيتم دعوة ضيف ليقدم نصائح عامة للطلاب حول «فن التعامل مع الضغوطات». أنت ضمن الفريق المسؤول عن اختيار الضيف، وبعد التحري عن الضيوف المرشحين، عُرِضت عليك المعلومات الآتية والتي تم جمعها من خلال تتبع البصمة الرقمية لكل ضيف، انظر الشكل (4-2).

المدرّب الثاني: يوسف

سيرته الذاتية:

- أخصائي نفسي حاصل على شهادة البكالوريوس من جامعة ...
- متطوع دائم في جمعيات تعنى بالصحة النفسية للمراهقين
- يعمل لدى مركز نفسي ويقدم استشارات خاصة

نتائج البحث عن المدرّب عبر الإنترنت

- لا يوجد لديه حسابات ظاهرة في وسائل التواصل الاجتماعي ماعدا حساب على (Linked In) يشارك فيه خبراته العلمية والعملية ويعيد نشر بعض المقالات العلمية.
- تقييمات الزوار له عبر المركز 4.2 من 5
- تعليقات بعض العملاء:
- تعليق 1: «اشكر الاخصائي المتميز يوسف لأخلاقه الراقية وحسن تعامله»
- تعليق 2: «موقع المركز بعيد جداً ويصعب الوصول إليه هذا بالإضافة للأسعار المبالغ فيها»

المدرّب الأول: محمد

سيرته الذاتية:

- مدرب معتمد حاصل على شهادة من المعهد العالمي للتطوير الشخصي
- خبرة 10 سنوات في مجال التدريب
- صدر له العديد من المؤلفات

نتائج البحث عن المدرّب عبر الإنترنت

- عدد المتابعين عبر تويتر 51k وعبر السناپ شات 1.2M وتم بيع أكثر من 10.000 نسخة من كتبه
- نتائج البحث عن المعهد العالمي لتطوير الشخصية: هو معهد افتراضي غير تابع لأي جهة رسمية
- مقال منشور:
- عنوان المقال: حقيقة المدرّب محمد «.... وادعى أحد المتابعين أن المادة المكتوبة في كتاب المدرّب الشهير محمد هي في الأصل كتاباته التي نشرها عبر صفحته على الفيس بوك وأرفق العديد من الصور التي تثبت ملكيته الفكرية للنص والتاريخ الذي يوضح وقت النشر..»
- عبر تويتر:
- إعجاب لتغريدات شخص يبث خطابات الكراهية عبر حسابه عبر تويتر.

شكل (4-2): معلومات الضيوف المرشحين لتقديم الدورة

ما وجهة نظرك الشخصية عن كل ضيف؟ ومن ستختار مع توضيح السبب؟



كل زميل في المجموعة يشارك أسبابه حول اختيار الضيف، سجل أهم النقاط التي شاركها زملاؤك.



راجع قراراتك مرة أخرى بعد الاستماع الى وجهات النظر الأخرى.
هل ساعدت آراء الزملاء على الإنتباه لجوانب أخرى قد تؤثر في قراراتك؟



قرارك النهائي:



لا شك أن للبصمة الرقمية أهمية كبيرة في العصر الحاضر، وأصبحت تصنف ضمن المعايير التي يُعتمد عليها في اتخاذ بعض القرارات المهمة، مثل:

■ القبول في الجامعات

تُحدث الجامعات سياسات القبول باستمرار عن طريق تحديد أفضل المعايير لقياس أهلية الطالب في ظل الإقبال والتنافس العالي من المتقدمين للدراسة في الجامعات من ناحية، وحرص الجامعات على رفع تقييمها لتكون في مصاف أفضل الجامعات العالمية. لذلك، تحرص الجامعات أن يكون طلابها مواطنين عقلانيين ويعبرون عن شخصيتهم من خلال السلوك الرقمي المسؤول سواء كان ذلك من خلال المدونات المكتوبة أو المسموعة أو المرئية، أو المحتوى على وسائل التواصل الاجتماعي، أو التعليقات عبر الإنترنت.

■ القبول في الوظائف

يستثمر أصحاب العمل الكثير من الوقت والمال في موظفيهم، وعملية التوظيف الآن أكثر تنافسية من أي وقت مضى؛ إذا كان من الممكن أن يُظهر بحث بسيط في محركات البحث أو في وسائل التواصل الاجتماعي أن المتقدم يشارك في مجتمعات إلكترونية ذات توجهات فكرية أو سياسية أو أخلاقية مخالفة للتوجهات الدينية والثقافية للمجتمع، أو يشارك في سلوك رقمي غير مسؤول، فهذا قد يؤدي إلى رفض قبول المتقدم في الوظيفة.

إثارة التفكير:



هل يوجد مجالات أخرى تظهر فيها أهمية البصمة الرقمية؟



وزارة التعليم

Ministry of Education

2023 - 1445

خطوات إدارة البصمة الرقمية

يوضح الشكل (5-2) مجموعة من الخطوات والتدابير التي يمكن أن تساعد في بناء وإدارة البصمة الرقمية:

راجع منشوراتك

من الجيد مراجعة المنشورات السابقة عبر الإنترنت وفي وسائل التواصل الاجتماعي وحذف غير المناسب منها

فكر قبل أن تنشر

المعلومات التي يتم مشاركتها عبر الإنترنت ستترك أثرًا دائمًا وينبغي للمستخدم ألا يقوم بنشر ما يمكن أن يُفهم بطريقة خاطئة أو يضر بسمعته

تحقق من المعلومات المتاحة عنك

من الجيد لمستخدم الإنترنت ووسائل التواصل الاجتماعي البحث كل بضعة أشهر في محركات البحث حول المعلومات المتاحة عنه حتى يكون على دراية بالمعلومات التي يمكن للآخرين الوصول إليها

لا تبالغ في المشاركة

ينبغي تجنب الإفراط في المشاركة وليكن الاهتمام بجودة المشاركة على حساب الكم

حذف الحسابات القديمة

لتقليل البصمة الرقمية من الأفضل حذف الحسابات القديمة على وسائل التواصل الاجتماعي وإلغاء الاشتراك في الرسائل البريدية للمواقع والأخبار التي لم يعد المستخدم مهتمًا بتلقي تحديثات منها

تحقق من إعدادات الخصوصية

تتيح إعدادات الخصوصية في وسائل التواصل الاجتماعي القدرة على التحكم في من يمكنه أن يرى المنشورات ومن يمكنه التعليق عليها، ينبغي مراجعة هذه الإعدادات وضبطها بما يتناسب مع احتياجات صاحب الحساب

شكل (5-2): خطوات إدارة البصمة الرقمية

تعد تنبيهات جوجل (Google Alert) إحدى الطرق للتحقق من المعلومات المتاحة عنك، من الجيد إعداد تنبيه حيث سترسل لك الأداة تنبيهات لكل منشور يحمل اسمك.



إضاءة



اقترح خطوات أخرى إضافية يمكن أن تساعد على إدارة البصمة الرقمية بطريقة إيجابية.

بصمتك الرقمية تؤثر على سمعتك الرقمية والتي بدورها ترتبط بشكل وثيق بسمعتك في العالم الواقعي. فيتعين عليك أن تتعلم كيف تدير بصمتك الرقمية. اعطني بها كنبته ترعاها من خلال مراجعة كل ما تنشر وتشارك لتقطف أطياب الثمر. قال تعالى: ﴿لَمْ تَرَ كَيْفَ ضَرَبَ اللَّهُ مَثَلًا كَلِمَةً طَيِّبَةً كَشَجَرَةٍ طَيِّبَةٍ أَصْلُهَا ثَابِتٌ وَفَرْعُهَا فِي السَّمَاءِ ۚ تُؤْتِي أُكْلَهَا كُلَّ حِينٍ بِإِذْنِ رَبِّهَا وَيَضْرِبُ اللَّهُ الْأَمْثَالَ لِلنَّاسِ لَعَلَّهُمْ يَتَذَكَّرُونَ ۝٢٥﴾



إضاءة

[سورة إبراهيم: 24-25]

|| السمعة الرقمية

تراكم البصمة الرقمية يؤدي إلى تكوين صورة ذهنية معينة عن الشخص لدى المتابعين وهو ما يطلق عليه السمعة الرقمية (Digital Reputation) بالتالي يمكن تعريف السمعة الرقمية بأنها:

الصورة الذهنية التي يبنها المتابع- أو ما يفكر به الناس ويعتقدونه- عن مستخدم شبكة الإنترنت بناءً على البصمة الرقمية التي يتركها عند استخدامه الشبكة.



1. السيناريوهات الآتية توضح نشاط كل من فرح وسلمان -البصمة الرقمية- في وسائل التواصل الاجتماعي، استنتج السمعة الرقمية لكل منهما؟

البصمة الرقمية	السمعة الرقمية
فرح: فتاة لديها حساب في برنامج التيك توك، تنشر عبر حسابها مقاطع ملهمة لتطوير الشخصية، اقتباسات من كتب، مع نصائح متنوعة في هذا المجال، كما أنها تقوم بالانضمام لمساحات نقاش في تويتر حول إستراتيجيات القراءة.	
سلمان: شاب لديه حساب في الانستغرام وينشر من خلاله وصفاته الخاصة لإعداد الطعام الصحي، ونصائح بخصوص بعض المكملات الغذائية التي تساعد في تحسين الصحة، كذلك ينشر بعض المقاطع عن فوائد الرياضة، كما يقوم من خلال حسابه بالإعجاب والتعليق والاشارة (Tags) لحسابات أشخاص آخرين مهتمين بالصحة والرياضة.	

2. فكر بشكل عكسي: ما هي البصمة الرقمية لأحمد؟

البصمة الرقمية	السمعة الرقمية
أحمد: محب للسفر واكتشاف الثقافات المختلفة	

3. تخيل أنك مدير شركة وتحتاج إلى موظفين في المجالات الآتية: التسويق، الموارد البشرية، العلاقات العامة، بافتراض أن (فرح، سلمان، أحمد) في السيناريوهات السابقة هم المتقدمين لهذه الوظائف ولديهم المؤهلات الأكاديمية لشغل هذه الوظائف. من ستختار لكل وظيفة؟ ولماذا؟

التسويق	الموارد البشرية	العلاقات العامة

اقترح مجموعة من السلوكيات الإيجابية عبر شبكة الإنترنت والتي قد تسهم في بناء سمعة رقمية إيجابية؟ وما السلوكيات السلبية التي قد تؤثر بشكل سيء على السمعة الرقمية؟

سمعة رقمية سلبية	سمعة رقمية إيجابية
.....	
.....	
.....	

سمعتك الرقمية هي بمثابة علامتك التجارية (your brand) والتي قد تؤثر بشكل كبير على حياتك في العالم الواقعي.



إضاءة

حماية السمعة الرقمية

قبل أن تشارك أي منشور عبر شبكة الإنترنت، اسأل نفسك الأسئلة الموضحة بالشكل (6-2):



شكل (6-2): طرائق حماية السمعة الرقمية

نشاط



اقترح طرقاً إضافية يمكن أن تساعد على حماية السمعة الرقمية.

غذاء الفكر



- كيف يراك الآخرون في العالم الرقمي - ما هي سمعتك الرقمية؟
- ما الشخصيات التي يمكن اعتبارها ذات سمعة سلبية من واقع متابعتك للعالم الرقمي؟
- ما الحد الفاصل بين مشاركة إنجازاتك ونجاحاتك وبين المبالغة في مشاركة ذلك؟



نقاط مهمة

- كل نشاط تقوم به في العالم الرقمي يضاف إلى بصمتك الرقمية وتراكم ذلك هو ما يبني هويتك وسمعتك الرقمية.
- ضع في اعتبارك كيف ستؤثر حتى أبسط المنشورات على سمعتك أو سمعة الآخرين الرقمية.
- لا تستخدم وسائل التواصل الاجتماعي للتدمير ونشر المشاعر السلبية والتقليل من شأن الآخرين.
- كن مفيداً وملهماً، وودوداً، ومتواضعاً.
- كن ذكياً في اختياراتك لمنشوراتك وخلقاً أثناء تواجدهم الرقمي.

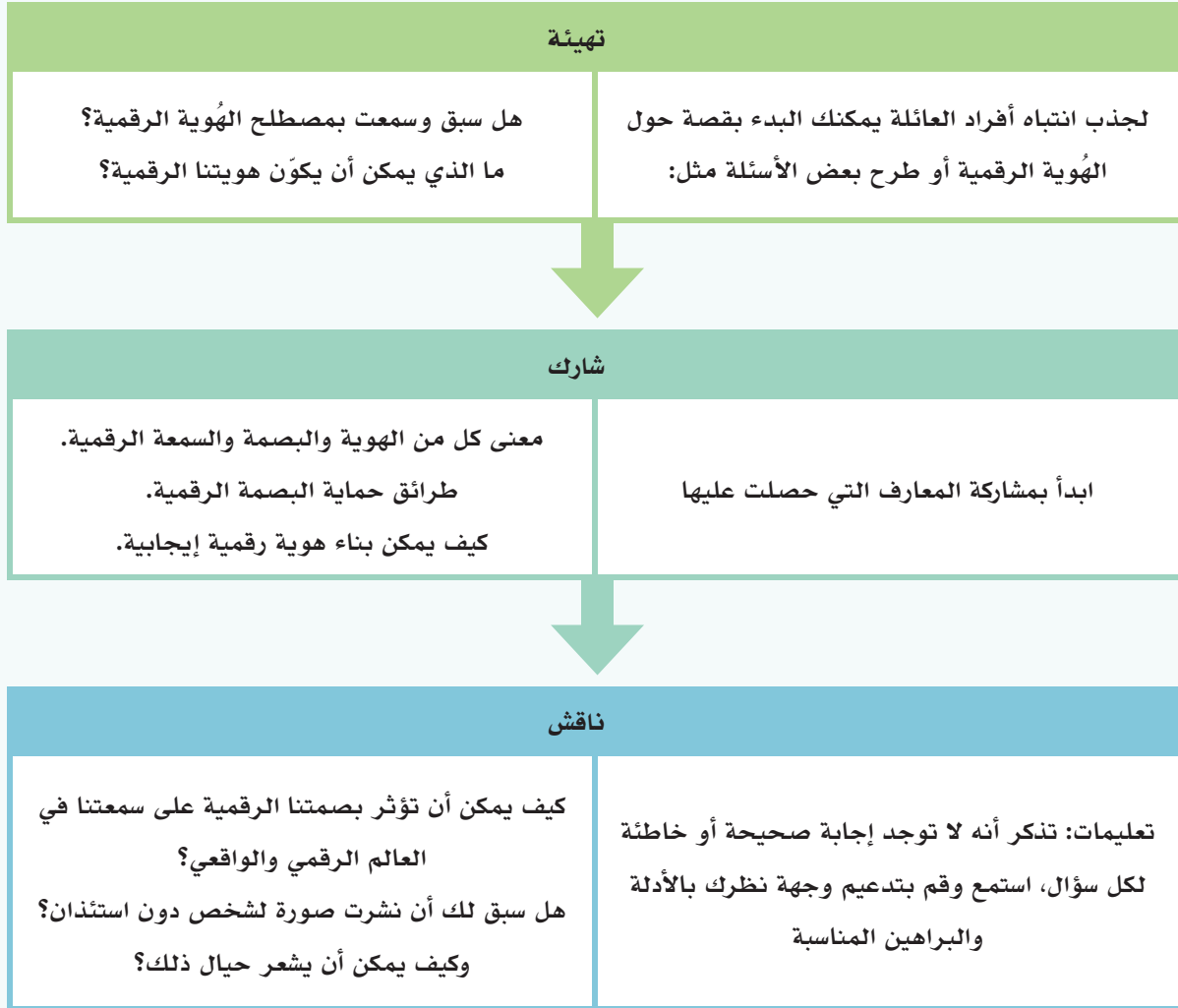


مشروع الدرس



لنشر الفائدة، شارك وناقش ما تعلمته حول الهوية والبصمة و السمعة الرقمية مع أفراد عائلتك.

1. للقيام بذلك، اتبع الخطوات الموضحة في الشكل (2-7):



شكل (2-7): خطوات عملية لمشاركة معلوماتك حول الهوية والبصمة و السمعة الرقمية مع أفراد الأسرة



2. اجمع الملاحظات من إجابات أفراد العائلة.

الملاحظات	أسماء المشاركين	الأسئلة (اكتب الأسئلة التي ترغب بطرحها أو مناقشتها مع أفراد العائلة)

3. اكتب تقريراً يوضح:

أ. كيف سارت العملية؟

ب. ردود أفعال أفراد العائلة وتفاعلهم مع الموضوع.

ج. إجابات بعض أفراد العائلة عن الأسئلة المطروحة.

د. تأملاتك في هذه الإجابات.





التواصل والعلاقات الرقمية

مخرجات التعلم:

- أتعرف على مفهوم آداب السلوك الرقمي وأهميته.
- أفرق بين السلوك الرقمي المسؤول، والسلوك الرقمي غير المسؤول.
- أستنتج آداب السلوك في التواصل الرقمي.
- أميز آداب السلوك الرقمي في منصة مدرستي.
- أناقش أهمية قيمة التعاطف في توجيه السلوك الرقمي المسؤول.
- أتعرف على مفهوم التواصل والعلاقات الرقمية.
- أعد قنات التواصل والعلاقات الرقمية.
- أميز بين العلاقات الرقمية الصحية والعلاقات الرقمية غير الصحية والعلاقات الرقمية الخطرة.
- أقترح حلولاً للتعامل مع العلاقات الرقمية الخطرة.
- أضع الحدود التي تجعل علاقاتي أفضل عبر الإنترنت.
- أتدرب على مهارات التواصل الرقمي الفعال.
- أتعرف على مفهوم الحوار المتحضر عبر الإنترنت وأهم مهاراته.
- أناقش التأثير السلبي لوسائل التواصل الاجتماعي على الأشخاص في مجال التواصل والعلاقات.



مصطلحات الدرس:

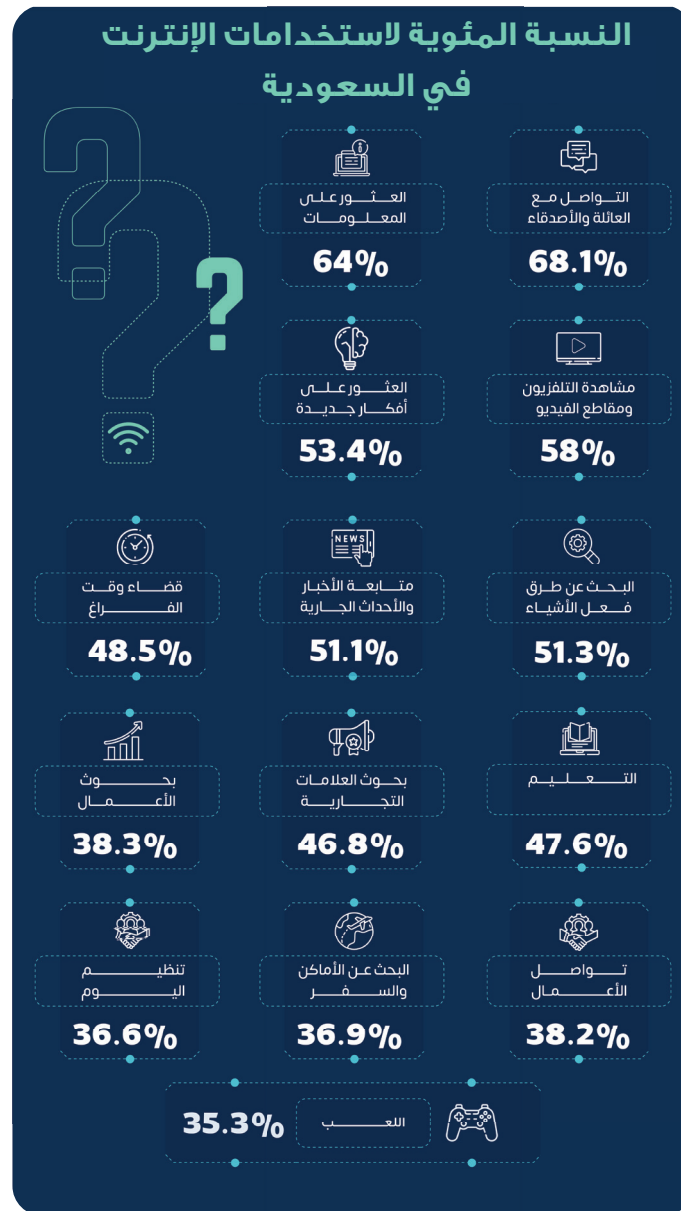
- آداب السلوك الرقمي (Netiquette).
- التحقير (Humiliating).
- السيطرة (Controlling).
- العلاقات الرقمية (Digital Relationships).
- التراص (Stalker).
- التعاطف في العالم الرقمي (Empathy).
- السلبية (Negativity).
- الابتزاز الإلكتروني (Online Blackmail).
- كشف الذات (Self-disclosure).
- الضغط (Pressure).
- تبديل نمط لغة الحوار (Code switching).
- التأييب (Blaming).
- الحوار المتحضر (Civil Discourse).

التهيئة

يعيش إنسان اليوم في عالم متصل، فبحسب الهيئة العامة للإحصاء في المملكة العربية السعودية فإن 93% من السكان في السعودية يستخدمون الإنترنت لأسباب مختلفة، منها التواصل وبناء العلاقات والمجتمعات الافتراضية، والعمل، والتعليم، والحصول على المعلومات والأخبار وغيرها من الأسباب. يحتل التواصل أعلى نسبة في استخدام الأفراد للإنترنت في السعودية كما هو موضح بالشكل (2-8)، وهذا التواصل والحضور الرقمي يستدعي التفكير في الآتي:

- ما الآداب والأخلاقيات اللائقة بالمواطن الرقمي؟
- هل يعكس سلوكي الرقمي هويتي الإسلامية والوطنية؟
- كيف تؤثر سلوكياتنا في العالم الرقمي على الآخرين؟
- من الأشخاص الذين أتواصل معهم باستخدام وسائل التواصل الاجتماعي؟
- كيف تؤثر وسائل التواصل الاجتماعي على حياتي؟





شكل (8-2): النسبة المئوية لأسباب استخدام الإنترنت في السعودية (2022)،

المصدر: شركة الاتجاه الرقمي للتطوير TREND

آداب السلوك الرقمي

السلوك الرقمي المسؤول يجعل كل مواطن مثلاً يحتذى به في حسن الخلق والتعامل حيث إن مستخدمو التقنية الرقمية، في الغالب، يتعلمون الآداب معاً من خلال سلوك الآخر، وهذا يحمل كل مواطن رقمي مسؤولية مراقبة سلوكه وضبطه. ويمكن تعريف آداب السلوك الرقمي (Netiquette) بأنها الأخلاقيات وقواعد السلوك للحوصل الإيجابي والفعال عبر شبكة الإنترنت لجعل العالم الرقمي مناسباً للجميع.

أهمية آداب السلوك الرقمي

- تكمُن أهمية الاتفاق على آداب عامه توجه السلوك الرقمي في الخصائص التي تميز هذا العالم والتي قد تجعل من تجربة التواجد الرقمي إيجابية أو سلبية بحسب سلوك المستخدم، ومن هذه الخصائص:
- أن التواصل الرقمي نصيٌّ في الغالب، حيث يخلو من استخدام لغة الجسد، وهذا قد يؤثر على جودة الاتصال بين المرسل والمتلقي.
- العالم الرقمي هو عالم ممتد ومتصل والمستخدمون هم أشخاص بخلفيات وثقافات مختلفة، فالمقبول لدى ثقافة ما قد يكون مرفوضاً عند ثقافة أخرى.
- سهولة الوصول للمواد المكتوبة والمرئية والمسموعة واستخدامها.
- صعوبة معرفة هوية الشخص المرسل، حيث تتيح شبكة الإنترنت ووسائل التواصل الاجتماعي للمستخدم إمكانية إخفاء هويته.
- إمكانية انتحال الشخصية والوصول غير المسموح به لمعلومات خاصة للمستخدمين الآخرين مما يعرضهم للأذى.
- فبدون وجود آداب توجه وتحكم السلوك الرقمي المناسب، قد يصبح العالم الرقمي مكاناً للتنمر، ونشر الشائعات، والإساءة للمستخدمين الآخرين، ولكل هذا تبعات قانونية يسببها الجهل وعدم الالتزام بقواعد آداب السلوك الرقمي.

إثراء



لكل منصة من شبكات التواصل الاجتماعي قواعد وسياسات تحكم سلوك المستخدمين، والإخلال بهذه السياسات قد يعرض صاحب الحساب لمشاكل منها إغلاق حسابه، أو حذف محتواه وقد تصل للمساءلة القانونية.

امسح رمز الاستجابة السريع للاطلاع على سياسات السلامة والخصوصية لكل من:

سناپ شات



يوتيوب



تويتر



آداب السلوك في التواصل الرقمي

يوجد العديد من الآداب والمبادئ الأساسية التي يجب على المواطن الرقمي الالتزام بها عند التواصل عبر شبكة الإنترنت، ومن أهم هذه الآداب والسلوكيات:

1. احترام خصوصية الآخرين من خلال عدم التواصل في أوقات غير مناسبة، أو مشاركة المعلومات الشخصية، أو الصور، أو مقاطع الفيديو التي لا يرغب الشخص الآخر في نشرها عبر شبكة الإنترنت.
2. احترام اختلاف الآخر بعدم التقليل منه أو تسفيه رأيه أو توجيهه.
3. احترام قواعد وقوانين حقوق الملكية الفكرية من خلال الإشارة للمصدر وعدم التعديل على الوسائط بما ينتهك حقوق المؤلف.
4. تحري الدقة والمصداقية عند النشر عبر الإنترنت.
5. تجنب تجاهل الرسائل المهمة وعدم التأخر في الرد ما أمكن.
6. تجنب نشر الشائعات والتعليقات التحريضية أو المسيئة عبر الإنترنت.
7. تجنب إرسال محتوى غير لائق دينياً أو أخلاقياً أو مجتمعياً.
8. تجنب الخوض في المواضيع المتعلقة بالعنصرية والطائفية والمثيرة للكرهية.
9. تجنب استخدام الألفاظ النابية والرد على التعليقات السلبية بالمثل لأنها قد تتحول إلى جريمة معلوماتية يحاسب عليها قانون مكافحة الجرائم المعلوماتية.
10. تجنب المشاركة أو التعليق بموضوع مختلف عن الموضوع المطروح من قبل صاحب المنشور.



من خلال السيناريوهات الآتية، اكتب السلوك الرقمي المسؤول وغير المسؤول الذي قد يقوم به المستخدم:

السلوك الرقمي غير المسؤول	السلوك الرقمي المسؤول	السيناريو
		يرغب محمد بإرسال بريد إلكتروني للمعلم يستفسر فيه عن الموعد النهائي لتسليم البحث
		التقطت مها صورة لها مع أحد الأقارب وترغب بمشاركتها عبر سناپ شات.
		قرأ خالد خبراً على أحد وسائل التواصل الاجتماعي ويرغب بمشاركته عبر تويتر لنشره على نطاق واسع.
		أنهت حنان دراسة مقرر ما وطُلب منها تقييم المقرر إلكترونياً من حيث المحتوى والمعلم المسؤول عن تقديمه.

آداب السلوك الرقمي في منصة مدرستي



حرصاً من وزارة التعليم على جعل تجربة التعليم الإلكتروني عبر منصة مدرستي تجربة ثرية وآمنة، أنشأت وزارة التعليم دليلاً إرشادياً لآداب السلوك الرقمي الواجب على الطلاب اتباعه، يوضح الشكل (2-9) آداب السلوك الرقمي، وللإطلاع على الدليل، امسح رمز الاستجابة السريع.



آداب السلوك الرقمي

 في حال الاستعانة بنص أو مصدر خارجي فإن توضيح للمراجع والمصادر والإشارة إليها يدل على احترامك لقوانين وحقوق الملكية الفكرية والنسخ.	 ابتعد عن المنصرية والطائفية والقبيلية البغيضة والقذف واللمز والانتقاص من الآخرين ومجهوداتهم	 حوارك مع الآخرين برقي وتقبل لأرائهم والنقد البناء يعبر عنك، لذلك أظهر الاحترام للطرف الآخر .	 اطلاعا على نظام مكافحة الجرائم الإلكترونية يمكنك من التعرف إلى المخالفات المرتبطة بالسلوك الرقمي.	 لا بد أن تظهر اتباع تعاليم وأداب الدين الإسلامي الحنيف والأعراف والتقاليد الوطنية السائدة في سلوكنا الرقمي ومشاركاتنا.
 لحفاظ على سرية بياناتك احرص على عدم نشر البيانات الشخصية كالأسماء وبيانات الاتصال والمناوين.	 لكل مقام مقال .. فاحرص دائما في الدرس الافتراضي والقنوات الرسمية على الابتعاد عن إرسال الصور أو الملصقات التعبيرية والاختصارات ووظفها أثناء مشاركتك الاجتماعية في ساحات النقاش.	 لكي تكون مشاركتك فاعلة لا بد أن تتسم بالجدية والمعلقة المباشرة بموضوع النقاش.	 احتراماً للفتن العربية لا بد من استخدام اللغة العربية الفصحى.	 احرص على تحري الدقة في نقل واستخدام الآيات القرآنية الكريمة والأحاديث النبوية الشريفة، والإشارة للمصدر من كتاب الله الكريم وكتب الصحاح.
 جهازك أمانة .. فاحرص على عدم فتح الروابط غير الآمنة والمجهولة، وتحقق من خلو الروابط والملفات من الفيروسات	 لتواصل فاعل أطلع الآخرين على المواعيد المناسبة لك للتواصل عبر المنصة وكذلك تعرف إلى مواعيدهم.	 كن قدوة في سلوكك الرقمي وانصح الآخرين بعدم إساءة استخدام أنظمة الوزارة للمشاركة الإلكترونية بما يؤثر على أدائها، أو مستوى أمانها، أو سرعتها، أو استمراريتها، أو حرمان الآخرين من الاستفادة منها.	 في حال تعرضت للهجوم من آخرين أو لنتنم الإلكتروني يجب عليك مشاركة المسؤولين هذه الحالة لاتخاذ اللازم .	 السلوك الرقمي سريع الوصول ولا يمكن التراجع عنه، فاحرص على ألا تترجم الغضب لردة فعل على المنصة،
 لأنكم أبطالنا وحرصاً عليكم نفيكم أن جميع مشاركات المستفيدين عبر المنصة محفوظة ويحق للوزارة الرجوع إليها عند الحاجة	 يفضل عدم استخدام قنوات التواصل غير الرسمية من الوزارة للتواصل مع المستفيدين الآخرين (مثل الواتس آب وغيره من تطبيقات التواصل الاجتماعي).	 التوقيت المثالي للرد على البريد الإلكتروني والاستفسارات المرسلة يكون خلال 24 ساعة من تاريخ الإرسال، وفي حال تطلب الرد وقتاً أطول يفضل إفادة الطرف الثاني بذلك احتراماً لتواصله معك.		

يحرص الأستاذ عادل معلم اللغة العربية على تفعيل أدوات التعليم الإلكتروني المتاحة عبر منصة مدرستي مثل: البث المباشر، وساحات النقاش بهدف إيجاد تجربة تعلم ثرية للطلاب.

1. بعد اطلاعك على الدليل الإرشادي للسلوك الرقمي (شكل 2-9) الصادر من وزارة التعليم، اكتب السلوكيات الإيجابية والمقبولة من الطلاب أثناء تواجدهم واستخدامهم للمنصة والسلوكيات السلبية التي قد تعيق سير الدرس.

سلوك رقمي إيجابي (مسؤول)	سلوك رقمي سلبي (غير مسؤول)
.....	
.....	
.....	
.....	

2. اقترح قوانين تساعد المعلم على ضبط السلوكيات غير المرغوبة من الطلاب أثناء استخدامهم للمنصة.

.....

.....

.....

|| التعاطف في العالم الرقمي لتعزيز السلوك الإيجابي

يقصد بالتعاطف في العالم الرقمي (Empathy) فهم شعور الآخر وما يفكر به قبل القيام بأي فعل أو ردة فعل أثناء التواصل الرقمي، فمع كثرة برامج التواصل وما تتطلبه من سرعة استجابة، ومع غياب رؤية رد فعل الطرف الآخر (المتلقي للمنشور) عن المشهد، يصبح من الصعب أخذ الوقت الكافي للتفكير في شعور الآخر تجاه ما يُنشر. ومن ذلك، تبرز أهمية التعاطف في العالم الرقمي كقيمة أساسية للمساعدة في توجيه السلوك الرقمي حيث إن التعاطف يقود إلى فهم اهتمامات الآخرين وشعورهم واحتياجاتهم ووجهات نظرهم؛ فيمكن اعتباره بمثابة بوصلة داخلية تساعد الشخص على توجيه سلوكه، ومكوّن ضروري لبناء مجتمعات رقمية أخلاقية. وقد أسس النبي الكريم لهذه القيمة فعن أنس بن مالك رضي الله عنه؛ أن النبي ﷺ قال: (لَا يُؤْمِنُ أَحَدُكُمْ حَتَّى يَحِبَّ لِأَخِيهِ مَا يُحِبُّ لِنَفْسِهِ) [صحيح البخاري، 19]. فما لا يرضاه الشخص ويقبله على نفسه ينبغي أن يتجنب فعله لشخص آخر وأن يُعامل الآخرين كما يحب أن يُعامل.

نشاط



اقترح بعض السلوكيات التي يمكن أن تساعد في تعزيز التعاطف في العالم الرقمي.

تدريب



مما درست، ما هي المعارف والقيم والمهارات الأساسية التي يحتاجها المواطن الرقمي ليكون ذا سلوك رقمي إيجابي.

	المعارف
	القيم
	المهارات



التواصل والعلاقات الرقمية

أحدثت ثورة الاتصالات والمعلومات تغييرات في طريقة التواصل بين الأفراد والمجتمعات، كما وسعت دائرة العلاقات لتكون ممتدة في أنحاء العالم عبر توفير مجموعة متنوعة من الوسائط والوسائل التقنية؛ والتواصل الرقمي (Digital Communication) عبارة عن تفاعلات متزامنة وغير متزامنة تحدث بين الأشخاص عبر شبكة الإنترنت، وتشمل التواصل عبر الصوت، والنص، والصورة، والفيديو، وتبادل المعلومات والملفات. أما العلاقات الرقمية (Digital Relationship) فيقصد بها العلاقات التي يتم التواصل بها عبر شبكة الإنترنت، وهي على شكلين:

1. علاقات يتم بناؤها عبر شبكة الإنترنت مثل الأصدقاء الرقميون الذين يتم التعرف عليهم من خلال ألعاب الفيديو عبر شبكة الإنترنت، أو المتابعين في وسائل التواصل الاجتماعي.
 2. استخدام وسائل التواصل الاجتماعي للتواصل مع أشخاص معروفين للمستخدم في العالم الواقعي.
- هذا التوسع في وسائل التواصل وإمكانية بناء العلاقات حمل معه العديد من المزايا والفوائد، إضافة إلى بعض الأخطار التي يجب التنبيه لها لتكون مواطناً رقمياً واعياً وصاحب تواجد مسؤول.

أنواع العلاقات الرقمية وأهميتها



شكل (2-10): أنواع العلاقات الرقمية وأهميتها

إثارة التفكير:



كيف يمكن أن تساعد العلاقات الرقمية في بناء بصمة وسمعة رقمية إيجابية؟

قنوات التواصل والعلاقات الرقمية

قنوات التواصل والعلاقات الرقمية



شبكات التواصل الاجتماعي



الألعاب الإلكترونية



مؤتمرات الفيديو



المدونات النصية والصوتية والمصورة



المنتديات



تقنيات الواقع المعزز، والواقع الافتراضي، والميتافيرس



شكل (11-2): قنوات التواصل والعلاقات الرقمية

يشير مصطلح «وسائل التواصل الاجتماعي» (Social Media) إلى التطبيقات والمواقع الإلكترونية التي تستخدم للتواصل مع الآخرين، ومن ضمنها المدونات النصية والمسموعة والمرئية، وشبكات مشاركة الوسائط، وشبكات المناقشة، وشبكات التواصل الاجتماعي (Social Network) مثل التيك توك والسناپ شات وتويتر.



إضاءة



العلاقات الرقمية الصحية والعلاقات الرقمية غير الصحية

نشاط



لكل منا تصوره عن العلاقات الصحية، في المربع الآتي اكتب الكلمات التي يمكن أن تصفها؟

يوضح الجدول (1-2) العديد من العلامات التي تدل على أن العلاقة الرقمية صحية أو غير صحية:

جدول (1-2): علامات العلاقات الرقمية الصحية وغير الصحية

العلاقات الرقمية غير الصحية	العلاقات الرقمية الصحية
تظهر فيها بعض أو كل العلامات الآتية:	تتميز العلاقات الصحية بـ:
• عدم التواصل	• التواصل الفعال
• عدم الاحترام	• الاحترام المتبادل
• عدم الثقة	• الثقة المتزنة
• قلة الدعم	• الصدق
• المبالغة في الغموض	• الدعم المتبادل
• محاولة الاستغلال	• الاستماع النشط
• كثرة اللوم والعتب	• حل الخلافات بهدوء
• الاستهزاء	



يارا طالبة في المرحلة الثانوية ونشطة في العديد من وسائل التواصل الاجتماعي. فيما يلي مثالين يوضحان بعض علاقاتها الرقمية.

سيناريو 1: يارا وموري -من اليابان- صديقات رقميات لأكثر من سنتين. موري تساعد يارا في تعلم اللغة اليابانية بينما يارا تساعد في تعلم اللغة العربية (تبادل اللغات). تبعد اليابان عن السعودية أكثر من 8 آلاف كيلومتر، ومع ذلك العلاقة بين يارا وموري لطيفة ومتينة حيث تتبادلان المعرفة والأخبار والتبريكات بالمناسبات.

سيناريو 2: تلقت يارا تنبيه عبر حسابها في تويتر عن استلامها رسالة من أحد المتابعات خلف معرف مجهول «ريم» في الرسائل الخاصة، ودارت المحادثة الآتية:



شكل (2-12): محادثة يارا مع «ريم» عبر الرسائل الخاصة

من السيناريوهات السابقة، وضح ما الفوائد التي يمكن أن تجنيها يارا من خلال هذه العلاقات وما الأخطار المحتملة.

الأخطار المحتملة	الفوائد

1. كيف تصف علاقة يارا وموري؟

2. كيف تصف علاقة يارا و «ريم»؟

3. ما سمعة يارا الرقمية؟

4. اقترح ردًا مناسبًا ليارا على سؤال «ريم» الأخير؟



أشكال العلاقات الرقمية الخطرة

1 الابتزاز الإلكتروني (ONLINE BLACKMAIL)

تخويف الشخص أو تهديده بكشف معلومات خاصة أو محرجة ونشرها عبر شبكة الإنترنت، والهدف منه التحكم بالشخص للقيام بأعمال غير قانونية، أو الحصول على المال، أو إجباره على فعل أمر ما يخالف الدين أو العرف المجتمعي.

2 الضغط (PRESSURE)

قيام شخص بالضغط على آخر عبر الإنترنت لفعل شيء لا يريد القيام به أو لا يشعر بالارتياح لفعله، يشمل ذلك الضغط في طلب إرسال صور غير لائقة عبر الإنترنت أو مشاركة معلومات خاصة.

3 التآنيب (BLAMING)

علاقة يقوم فيها أحد الأطراف بلعب دور الضحية بشكل دائم ويحرص على أن يشعر الطرف الآخر بالذنب لكل تصرف يقوم به.

4 التحقير والإهانة (HUMILIATING)

تلقي الشخص تعليقات سلبية أو انتقادات علنية من شخص آخر عبر شبكة الإنترنت يعتمد أن يحط من قدره، إما بالتقليل من شأنه أو التقليل من قدراته أو التقليل من إنجازاته.

5 السيطرة/ التحكم (CONTROLLING)

عندما يتحكم شخص في كيفية تفاعل شخص آخر عبر شبكة الأنترنت، كأن يطلب منه إلغاء متابعة شخص ما، أو حذف تعليق، أو عدم استخدام أحد وسائل التواصل.

6 التردد (STALKER)

أن يتابع شخص مستخدم آخر على جميع حساباته الرقمية بقصد مراقبته وتتبع نشاطاته ومعرفة جميع تحركاته لأسباب منها مقابله في الواقع أو هوس شخصي لديه تجاه هذا الشخص أو لابتزازه أو تهديده.

7 السلبية (NEGATIVITY)

شخص يغلب على منشوراته الشؤم والسلبية ويحاول غالباً إيجاد العيب في كل ما يُنشر.

شكل (2-13): أشكال العلاقات الرقمية الخطرة

«مكافحة الابتزاز» هي خدمة إلكترونية تقدمها الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر تمكن من مكافحة تهديد شخص أو ابتزازه، وتتعامل الهيئة بمنتهى السرية والخصوصية والاحترافية مع كافة الحالات. فعند التعرض للتهديد أو الابتزاز لابد من:

- حفظ الأدلة التي تثبت التعرض للابتزاز (لقطات شاشة، تسجيل صوتي، صور، مقاطع مصورة).
- حظر الحساب الذي يقوم بعملية الابتزاز وعدم التجاوب معه.
- الإبلاغ عبر:

- الاتصال: رقم مكافحة الابتزاز الموحد 1909، رقم مكافحة الابتزاز الدولي 0096611490666
- موقع «كلنا آمن»
- الموقع الإلكتروني الخاص بمكافحة الابتزاز، يمكن الوصول للموقع عبر مسح رمز الاستجابة السريع



نشاط



الحالات الآتية توضح أمثلة لعلاقات رقمية خطيرة، بالتعاون مع زملائك اكتب نوع العلاقة الخطرة ثم اقترح حلولاً مناسبة للتعامل مع كل حالة.

الحالة	نوع العلاقة الخطرة	الحل المناسب للتعامل مع العلاقة الخطرة
أن يلح شخص بطلب صور أو مقاطع مصورة بعد رفض الطرف الآخر القيام بذلك		
التعليق بضحك واستهزاء وبشكل علني على الصورة الشخصية لصديق في أحد وسائل التواصل الاجتماعي		
أن يستلم شخص صورة لباب منزلة من مجهول على أحد وسائل التواصل مع تعليق يوضح معرفة هذا المجهول بكل تحركاته		
أن يطلب شخص من آخر مبلغ مالي مقابل عدم نشر رسائل خاصة عبر الإنترنت		



أثناء خلوتك مع هاتفك الذكي أو أي جهاز إلكتروني استحضر معنى الإحسان وهو أن تعبد الله كأنك تراه فإن لم تكن تراه فإنه يراك، فغياب الحضور الواقعي في العلاقات الرقمية لا يعني أنه بإمكانك قول أو فعل ما تريد، وتذكر أن الله امتدح المتقين وأحبهم، قال تعالى: ﴿وَلَمَنْ خَافَ مَقَامَ رَبِّهِ جَنَّاتٍ﴾ [سورة الرحمن: 46]

أ. حدود التواصل في العلاقات الرقمية

يوضح الجدول (2-2) الحدود التي ينبغي على المواطن الرقمي المسؤول الالتزام بها للاستفادة من خصائص التواصل والعلاقات الرقمية وتجنب أخطارها:

جدول (2-2): حدود التواصل في العلاقات الرقمية

تجنب	افعل
1. كشف الذات (Self-disclosure) وهو أن يكشف الشخص أو يشارك معلومات، صور، أو فيديوهات خاصة، أو محرجة عن نفسه أمام الآخرين.	1. كن سفيراً للدين والوطن من خلال الاعتزاز بالهوية الإسلامية والوطنية وإبراز دور المملكة الإيجابي وتقديمها على جميع الأصعدة.
2. إرسال رسائل نصية إلى الأصدقاء على مدار الساعة وطوال أيام الأسبوع.	2. في حالة المرور بموقف تشعر فيه بعدم الارتياح أو الضغط أو الغضب تذكر القاعدة الذهبية «توقف»، «تفكر» ثم «تصرف».
3. فتح هاتف صديق أو قراءة رسائله الخاصة دون إذن منه.	3. ارسم حدوداً مع الآخرين بشكل واضح والتزم بها.
4. التحدث في الأمور الخاصة أو الشخصية أو العائلية مع الغرباء.	4. عند حدوث خلاف بسبب عدم وضوح الفكرة، استدرك سوء الفهم وبادر بالاعتذار والتوضيح.
5. الإشارة إلى الأصدقاء (Tags) بدون إذنه.	5. عند الحاجة، خذ استراحة من وسائل التواصل الاجتماعي لإعادة ترتيب العلاقات والأولويات.
6. تسجيل الإعجاب وإعادة مشاركة كل ما ينشره الأصدقاء.	6. عند التعرض لتهديد أو ابتزاز تحدث إلى الأشخاص الثقة (أحد الوالدين، المرشد الطلابي، أحد معلميك، الجهات الحكومية المختصة).
7. نشر تعليقات سلبية أو فيها إساءة للآخرين على وسائل التواصل الاجتماعي.	
8. كشف جدال خاص بشكل علني على أحد وسائل التواصل الاجتماعي.	
9. نشر شائعة عن زميل دراسة على وسائل التواصل الاجتماعي.	



خالد ويوسف زميلا دراسة وعلاقتهم جيدة؛ مؤخراً بدأ خالد في إرسال الكثير من الرسائل إلى يوسف -كل يوم وفي أي وقت- وكان خالد يغضب إذا لم يجد تفاعلاً ورداً سريعاً؛ يعتقد يوسف أن الوقت قد حان لوضع بعض الحدود لخالد من أجل استمرار صداقتهم، ولكنه في الوقت نفسه لا يريد أن يؤذي مشاعر صديقه بأي شكل. اقترح حلولاً تساعد يوسف في كيفية التعامل مع الموقف.

التواصل الرقمي الفعال

- هناك مجموعة من المهارات التي يمكن أن تساعد على رفع جودة التواصل عبر وسائل التواصل الاجتماعي. منها:
1. تفعيل مهارات الذكاء العاطفي أثناء التواصل مع الآخرين، ومن الوسائل المساعدة على إظهار المشاعر في العالم الرقمي: الرموز التعبيرية (emojis)، الصور، ومقاطع الفيديو.
 2. مراعاة آداب السلوك الرقمي.
 3. مراعاة آداب الخصام والاختلاف، ومنها:
 - مراقبة الله عز وجل في الخصومة.
 - ضبط اللسان.
 - حفظ القلب والنفس من تبعات الخصومة.
 - المبادرة بالاعتذار في حالة الخطأ.
 4. مهارة تبديل نمط لغة التواصل: غالباً يعتمد ما نقوله وكيف نقوله على الجمهور المستهدف بتلقي الرسالة، فالطريقة التي يتم التواصل بها مع الأصدقاء عبر شبكة الإنترنت لا بد وأن تكون مختلفة تماماً عن الطريقة التي يتم بها التواصل مع معلم المدرسة. وهذا يسمى تبديل نمط لغة التواصل (Code-Switching) ويقصد به تبديل الأسلوب المستخدم في التواصل اعتماداً على مع من تتواصل أو وسيلة التواصل التي يتم استخدامها.



فوائد تبديل نمط لغة التواصل:

- تمكن المستخدم من التواصل بطريقة يفهمها المقصود بالرسالة بشكل أفضل.
- تساعد في بناء علاقات إيجابية.
- تساعد في تجنب سوء الفهم الناتج عن أسلوب ونمط التواصل.

تدريب



تأمل في طريقة تواصلك مع الأهل والأصدقاء، المتابعين في وسائل التواصل الاجتماعي، معلم المدرسة. كيف يمكن أن تفعل مهارة تبديل نمط اللغة مع كل منهم من أجل رفع جودة تواصلك؟

الأهل والأصدقاء	المتابعين عبر الإنترنت	معلم المدرسة

الحوار المتحضر في العالم الرقمي

لا شك أن التواصل عبر شبكة الإنترنت أصبح قوة مؤثرة يمكن أن تستخدم بطريقة إيجابية أو سلبية من خلال التأثير في الرأي العام أو القيام بتغيير من خلال الحملات التي يتم تنظيمها أو المشاركة بها عبر وسائل التواصل الاجتماعي والتي تستخدم فيها الوسوم غالبًا (Hashtags)؛ والمشاركة في مثل هذه المنصات يتطلب أخلاقيات عالية تعكس هوية الشخص الإسلامية والوطنية والحرص على دعم القضية التي يشارك بها، وهذا ما يمكن أن يطلق عليه الحوار المتحضر (Civil discourse) ويقصد به الحوار المثمر الذي يسمح للناس بالاستماع إلى الآراء المختلفة والتعبير عن آرائهم بطريقة محترمة والتوصل إلى تفاهم مشترك.



يوضح الشكل (2-14) أهم المهارات للمشاركة في الحوار المتحضر:



شكل (2-14): مهارات تعزيز الحوار المتحضر عبر الإنترنت

وأثناء المشاركة في مثل هذه الحوارات، طبق سياسة الميمات الخمس شكل (2-15)، كن:

مراقباً الله	فكر قبل أن تنشر وتذكر معية الله لك في السر والعلن
مسترخياً	خذ نفساً عميقاً واسترخي قبل المشاركة في النقاش
منفتحاً	ضع في اعتبارك أهمية تفهم الأفكار التي تختلف عن أفكارك
مركزاً على الأفكار	ركز على نقاش الفكرة وتجنب التشتت والانتقال من موضوع لآخر
متابعاً ومستمعاً نشطاً	احرص على فهم أفكار الأشخاص الذين تتحاور معهم والخبرات التي مروا بها، بدلاً من التركيز على الرد فقط

شكل (2-15): الميمات الخمس للمشاركة في حوار متحضر

التأثير السلبي لوسائل التواصل الاجتماعي في مجال التواصل والعلاقات

مما تقدم، يظهر التغيير والفوائد التي أحدثتها وسائل التواصل الاجتماعي والمجتمعات الرقمية في مجال التواصل والعلاقات؛ ولكن في المقابل هناك بعض السلبيات الناتجة عن استخدام الوسائل الرقمية للتواصل، منها:

1. التأثير سلباً على قدرة الأشخاص على استخدام لغة الجسد والتواصل البصري بشكل فعال في مواقف الحياة الواقعية؛ ويرجع ذلك لكثرة الاعتماد على النصوص والصور في هذه الوسائل الرقمية.
2. ضعف مستوى لغة التواصل بسبب الاعتماد على بعض الاختصارات والكلمات المتداولة في وسائل التواصل الرقمية.
3. تفضيل العزلة وقضاء الوقت مع العلاقات الرقمية بدل الانخراط في العالم الواقعي.
4. نقص تقدير الذات وظهور مشاكل نفسية مثل القلق والاكتئاب بسبب المقارنة مع الأشخاص الآخرين في وسائل التواصل المختلفة.
5. إمكانية التعرض للتنمر والتحرش الإلكتروني.

نشاط



حياتي الرقمية:

1. فكر بعمق بعلاقاتك الرقمية واستخدم الشكل (16-2) لكتابة تأملاتك.
2. شارك تأملاتك مع أحد زملائك.



البرامج والتطبيقات التي أستخدمها بكثرة



أنشطتي الرقمية التي تخص التواصل والعلاقات



أصنف أنواع علاقاتي الرقمية



بعض الأمور التي تقلق والدي أو لا تعجبهم في حياتي الرقمية



بعض الأمور التي تقلقني أو لا تعجبني في علاقاتي الرقمية



كيف يمكن أن أتصرف إذا واجهت موقفًا مزعجًا في أحد وسائل التواصل الاجتماعي؟



ما الذي يمكنني فعله لجعل علاقاتي وحياتي الرقمية أفضل؟



شكل (2-16): حياتي الرقمية

غذاء الفكر

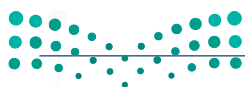


- «الكلمة قوة» كيف يمكن أن توظفها؟
- هل يلزمك المشاركة في الحملات والنقاشات المختلفة عبر شبكة الإنترنت؟
- لو أردت التخفيف من وسائل التواصل الاجتماعي أيها ستختار، ولماذا؟



نقاط مهمة

- احفظ طاقتك، فليس كل نقاش يستحق مجهودك.
- قل خيرًا أو اصمت.
- كن خير سفير لدينك ووطنك بتواجدك الرقمي المسؤول.
- بين فترة وأخرى راجع قائمة علاقاتك الرقمية وتأكد أنها تناسب قيمك ومبادئك.



مشروع الدرس



اختر أحد المشروعات:

1. مشروع فردي: باستخدام شبكة الإنترنت ابحث عن قصة واقعية لأحد أشكال العلاقات الرقمية الخطرة. ثم قم بالآتي:

- كتابة ملخص القصة.
- تحليل القصة: الأسباب التي أدت إلى تورط الشخص بعلاقة رقمية خطيرة، دوافع الشخص المستهدف، وتداعيات العلاقة الخطرة.
- اقترح طرقاً تساعد المتورطين في علاقة رقمية خطيرة مشابهة للقصة على حماية أنفسهم والتخلص من العلاقة.
- كيف يمكن تجنب مثل هذه العلاقة.
- صمم عرضاً مرئياً لبحثك واعرضه على المعلم والزملاء في الفصل.

2. نشاط مجتمعي: بالتعاون مع زملائك، صمم رسم معلوماتي (Infographic) توعوي يلخص أحد المواضيع في الدرس.

- أ. اختر أحد موضوعات الدرس (مثل: آداب السلوك الرقمي، أنواع العلاقات الرقمية، الحوار المتحضر).
- ب. لخص أهم الأفكار حول الموضوع المتفق عليه من قبل أعضاء المجموعة.
- ج. صمم رسماً معلوماتياً.
- د. اعرضه على المعلم والزملاء.
- هـ. قم بنشره.



العنف الإلكتروني

رابط الدرس الرقمي



www.ien.edu.sa

مخرجات التعلم:



- أتعرف على مفهوم العنف الإلكتروني وبعض أشكاله.
- أتعرف على مفهوم كل من الدراما الرقمية، والتنمر الإلكتروني، وخطاب الكراهية عبر الإنترنت.
- أفرق بين أشكال العنف الإلكتروني.
- أحلل الأسباب التي تؤدي لحدوث أو تصعيد الدراما الرقمية، والتنمر الإلكتروني، وخطاب الكراهية عبر الإنترنت.
- أستنتج أشكال التنمر الإلكتروني.
- أناقش آثار كل من الدراما الرقمية، التنمر الإلكتروني، وخطاب الكراهية عبر الإنترنت على الأفراد والمجتمعات.
- أتعرف على دوافع التنمر الإلكتروني.
- أطبق بعض الحلول للتعامل مع الدراما الرقمية، والتنمر الإلكتروني، وخطاب الكراهية عبر الإنترنت.
- أميز دور وسائل التواصل الاجتماعي في زيادة الدراما الرقمية، والتنمر الإلكتروني، وخطاب الكراهية عبر الإنترنت.
- أتعرف على جهود المملكة العربية السعودية للحد من أشكال العنف الإلكتروني.
- أشارك في التوعية بأشكال العنف الإلكتروني وسبل الوقاية منه.

مصطلحات الدرس:

- العنف الإلكتروني (Cyber Violence)
- الدراما الرقمية (Digital Drama)
- التنمر الإلكتروني (Cyberbullying)
- خطابات الكراهية عبر الإنترنت (Online Hate Speech)
- الإقصاء (Exclusion)
- المضايقة (Trolling)
- المطاردة الإلكترونية (Cyber stalking)
- الخداع (Trickery)
- التشويه (Denigration)
- انتحال الشخصية (Frapping)

التهيئة

الكرامة الإنسانية حق مكفول من الله عز وجل لجميع البشر. وقد نصت الشريعة الإسلامية على أهمية حفظ اللسان وعدم تتبع عورات المسلمين وإيذائهم بالقول أو الفعل، قال تعالى: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا يَسْخَرْ قَوْمٌ مِّنْ قَوْمٍ عَسَىٰ أَن يَكُونُوا خَيْرًا مِّنْهُمْ وَلَا نِسَاءٌ مِّنْ نِّسَاءٍ عَسَىٰ أَن يَكُنَّ خَيْرًا مِّنْهُنَّ وَلَا تَلْمِزُوا أَنْفُسَكُمْ وَلَا تَنَابَزُوا بِالْأَلْقَابِ بِئْسَ الْأَسْمُ الْفُسُوقُ بَعْدَ الْإِيمَانِ وَمَن لَّمْ يَتُبَّ فَأُولَٰئِكَ هُمُ الظَّالِمُونَ﴾ [الحجرات: 11]، وعن أبي برزة الأسلمي، قال: قال رسول الله ﷺ: (يا معشر من آمن بلسانه ولم يدخل الإيمان قلبه، لا تغتابوا المسلمين، ولا تتبعوا عوراتهم؛ فإنه من اتبع عوراتهم يتبع الله عورته، ومن يتبع الله عورته يفضحه في بيته) [صحيح أبي داود، 4880]

بالرغم من الفوائد الجمة للتقنية الرقمية إلا أن البعض قد يستخدمها بطريقة خاطئة قد تصل لتعنيف الآخر:

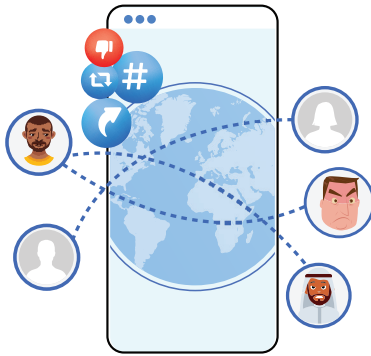
- هل سبق وأن تعرضت للتنمر الإلكتروني؟ وكيف تعاملت مع الموقف؟
- كيف تتعامل مع المنشورات المسيئة للآخرين؟
- ما دورك كمواطن رقمي في الحد من أشكال العنف الإلكتروني؟

العنف الإلكتروني

يشير العنف الإلكتروني (Cyber Violence) إلى استخدام التقنية الرقمية للتسبب بأذى جسدي أو نفسي أو مالي يستهدف الأفراد أو المنظمات أو المجتمعات. ويوجد العديد من أشكال العنف الرقمي ومنها:

- الدراما الرقمية.
- التنمر الإلكتروني.
- خطاب الكراهية عبر الإنترنت

الدراما الرقمية



تشير الدراما الرقمية (Digital Drama) إلى بعض أشكال الردود السلبية والمضايقات التي تحدث في الفضاء الرقمي عندما يستخدم الأفراد وسائل التواصل الاجتماعي لبدء أو زيادة جدال أو شجار بين مجموعة من الأشخاص. قد يكون هذا الشجار متصلًا بموقف واقعي ويتم تصعيده من خلال وسائل التواصل الاجتماعي، أو قد يبدأ من خلال المنصات الرقمية.

نشاط



ستقيم المدرسة حفلًا للخريجين، وقد كلف المعلم طلابه ترشيح من يرى في نفسه القدرة على الإلقاء، وتم اختيار سالم لهذه المهمة. شارك سالم الخبر مع متابعيه عبر تطبيق التيك توك من خلال مقطع مصور يوضح فيه سعادته لاختياره لتقديم كلمة الخريجين.

فيصل: مبارك سالم 😊

مجهول: حقيقة خالد هو من يستحق أن يكون الممثل للطلاب ومن يلقي كلمة الخريجين، ونعلم جميعًا لماذا قام

المعلم باختيار سالم (المفضل عند المعلمين) 😊

أحمد: شيء مؤسف 🗨️ والمشكلة أن أسلوب سالم سيء في الإلقاء.

محمد: مدرستنا الموقرة ***** @ نريد #خالد - ممثل - للخريجين

يوضح هذا السيناريو شكلاً من أشكال الدراما التي يمكن أن تتصاعد بسبب موقف ما وردة الفعل على هذا الموقف،
المطلوب:

1. لعب الأدوار: في مجموعتك، سيتبنى كل طالب وجهة نظر شخص من السيناريو السابق: سالم، فيصل، المجهول، أحمد، محمد. اكتب اسم الشخص الذي اخترته في الفراغ، ثم بناءً على هذا المنظور، اكتب الأسباب التي جعلتك تتصرف بهذه الطريقة.

● الشخص الذي اخترته هو

● السبب لتصرفي بهذه الطريقة هو

2. ناقش مع مجموعتك:

● الأسباب المحتملة لمثل هذه التصرفات.

● الأطراف الذين يمكن أن يتأثروا بهذه الدراما غير المذكورين في السيناريو؟

3. فكر ثم اكتب، ما التصرف الصحيح الذي يمكن أن تقوم به الشخصية التي اخترتها لجعل الموقف أفضل؟



العوامل التي تساعد على حدوث الدراما الرقمية

تساعد طبيعة شبكة الإنترنت في تقديم وسائل تساعد في تصعيد الدراما الرقمية للأسباب الموضحة في الشكل (17-2):



شكل (17-2): العوامل المساعدة على تصعيد الدراما الرقمية

نشاط



بالرجوع إلى النشاط السابق (17-2)

1. حلل الموقف واستنتج العوامل التي ساعدت في تصعيد الدراما الرقمية؟

2. تخيل استمرار تتالي الردود على المنشور السابق، ما الآثار التي قد تتركها الدراما الرقمية على الأفراد المشاركين؟



آثار الدراما الرقمية

الدراما الرقمية واسعة الانتشار وقد تكون أكثر صعوبة في تمييزها من أشكال العنف الإلكتروني الأخرى، ومع ذلك فهي تترك آثار سلبية على الأشخاص المشاركين في تصعيد الدراما، يوضح الشكل (2-18) بعض من تلك الآثار:

آثار الدراما الرقمية

- 1 قد تؤثر على السمعة الرقمية.
- 2 قد تؤدي إلى أضرار نفسية.
- 3 قد تؤدي إلى فقدان الثقة بالآخرين وقطع العلاقات.
- 4 قد يمتد أثرها ليشمل أفراد غير معنيين بشكل مباشر بالدراما مثل الأهل.
- 5 قد تتحول إلى صراع لفظي أو جسدي على أرض الواقع.
- 6 قد تتصاعد إلى أحد أشكال التنمر الإلكتروني أو تتحول إلى خطاب يبعث الكراهية.

شكل (2-18): الآثار السلبية للدراما الرقمية

كيفية التعامل مع الدراما الرقمية

في كل حدث درامي يحصل عبر شبكة الإنترنت يمكن أن يتخذ الشخص موقف إيجابي في تقليل حدة الصراع والخلاف، أو دور سلبي عبر تصعيده. يعرض الجدول (2-3) بعض الطرق الفعالة للتخفيف من تصعيد الدراما الرقمية:



جدول (2-3): كيفية التعامل مع الدراما الرقمية

لا تفعل	افعل
● الرد على الرسائل غير اللائقة. ● إعادة إرسال ونشر الشائعات. ● تصديق كل ما يتم نشره وتداوله بدون تحقق. ● تصعيد المشكلة من خلال الردود السلبية.	● تجاهل المنشور. ● المشاركة بتعليق إيجابي للتخفيف من حدة التصعيد. ● إذا كان ذلك ممكناً، التحدث مع الأطراف المشاركين في الدراما الرقمية وجهاً لوجه لمحاولة تهدئة الموقف. ● عند المشاركة، دقق الرسالة وفكر قبل النشر. ● احترام الرأي والرأي الآخر.

تدريب



السيناريو الأول: نشرت المدرسة مقالاً إلكترونياً عن المبادرة التي قامت بها الطالبات في اليوم العالمي للحفاظ على البيئة مع تضمين صور من بعض أعمال الطالبات المشاركات في التوعية بهذا اليوم، وأعدت إحدى الطالبات مشاركة المقال عبر صفحتها الإلكترونية مع تعليق يستفسر عن السبب في عدم تضمين صور لأعمال بقية الطالبات المشاركات أو أسمائهن ضمن المقال المنشور.

السيناريو الثاني: أرسل طلال مقطع فيديو ساخر لمجموعة الواتساب أثناء تسجيل الفريق الكروي الذي يشجعه هدف الفوز على الفريق الآخر مما استفز بعض أعضاء المجموعة المشجعين للفريق الآخر. كيف يمكن تصعيد الدراما الرقمية أو تخفيف حدتها في كل من السيناريوهات السابقة.

النص	تصعيد الدراما الرقمية	تخفيف حدة الدراما الرقمية
الأول		
الثاني		



التنمر الإلكتروني



يُعرّف التنمر الإلكتروني (Cyberbullying) بأنه سلوك متعمد يهدف إلى إخافة أو استفزاز الأشخاص المستهدفين أو تشويه سمعتهم، ويحدث باستخدام الأجهزة الرقمية عبر وسائل التواصل الاجتماعي أو الألعاب الإلكترونية حيث يمكن للأشخاص عرض المحتوى أو التعليق عليه أو مشاركته. ومن سلوكيات التنمر الإلكتروني:

- إرسال، أو نشر، أو مشاركة محتوى سلبي، أو ضار، أو كاذب أو فيه إهانة متعمدة وعلنية لشخص آخر، كمشاركة معلومات شخصية أو خاصة أو مفبركة.
- إرسال رسائل تهديد لشخص آخر.
- انتحال شخصية شخص ما، وإرسال رسائل مسيئة للآخرين.

نشاط



1. اقرأ السيناريوهات الآتية وحدد ما إذا كان النص يدل على حدوث تنمر إلكتروني أم لا:

السيناريو الأول: قامت أحلام بحفظ صورة شخصية لنوره نشرتها عبر قصتها في السناش دون إذن سابق، ثم شاركت الصورة بعد التعديل عليها لتبدو بشكل مضحك في مجموعة خاصة بصديقاتها، وتناقلت التعليقات السلبية والساخرة من أعضاء المجموعة، وصلت الصورة لنوره التي حزنت كثيراً عند رؤيتها وقراءة التعليقات. هل يعد هذا تنمر إلكتروني؟ ما الذي يمكن لنوره فعله؟

السيناريو الثاني: يلعب سلطان مع صديقه علاء لعبة إلكترونية عبر شبكة الإنترنت، يُبدي علاء بين فترة وأخرى تعليقاً ساخراً على طريقة لعب سلطان. هل يعتبر هذا تنمر إلكتروني؟ ما الذي يمكن لسلطان فعله؟



السيناريو الثالث: حصل خلاف بين خالد وأحمد، وعبر خالد عن غضبه من خلال إرسال عبارات بذيئة عبر الواتساب ثم قام بحظر رقم أحمد.

هل يعتبر هذا تنمر إلكتروني؟ ما الذي يمكن لأحمد فعله؟

.....

2. بعد قراءة السيناريوهات السابقة، ناقش مع زملائك ما الفرق بين المزاح، الإساءة، والتنمر في العالم الرقمي؟

.....

.....

أشكال التنمر الإلكتروني

تختلف أشكال التنمر الإلكتروني ويختلف مدى الأثر الذي يمكن أن تتركه على الشخص المستهدف، يوضح الشكل (19-2) بعض أشهر أشكال التنمر الإلكتروني:

المطاردة الإلكترونية Cyber stalking

مراقبة الشخص المستهدف وتتبعه إلكترونياً ومحاولة جمع كل المعلومات عنه، قد تكون مصحوبة بمطاردة واقعية وقد تمتد لتهديد المستهدف.

المضايقة Trolling

الإساءة للآخرين عاطفياً عن طريق الإهانة والسخرية أو التقليل من شأنهم بشكل متعمد، غالباً بهدف المتعة فقط.

الإقصاء Exclusion

استبعاد أو عزل شخص ما بشكل متعمد من بعض الأنشطة الجماعية عبر الإنترنت بهدف مضايقته وإزعاجه.

الخداع Trickery

كسب ود الشخص المستهدف وثقته حتى يشارك معلومات أو صور شخصية أو سرية، ثم يقوم المتنمر بفضح المتنمر عليه عن طريق كشف هذه المعلومات.

التشويه Denigration

تعتمد تشويه سمعة المتنمر عليه عن طريق نشر الشائعات وإرسال معلومات خاطئة ومضربة ونشرها عبر الإنترنت.

انتحال الشخصية Fraping

الدخول لحساب المتنمر عليه إما باختراقه أو من خلال معرفة كلمة السر ونشر صور مسيئة ومحتوى مؤذي.



شكل (19-2): أشكال التنمر الإلكتروني

صنف السيناريوهات الآتية بحسب أنواع التنمر الإلكتروني:

نوع التنمر	مثال
	سعت سلمى للتقرب من هالة لمعرفة سبب فقدانها الملحوظ لوزنها، وبعد عدة محاولات صارتها هالة بإصابتها بمرض فقدان الشهية العصبي (Anorexia nervosa)، بعد ذلك علّقت سلمى على أحد منشورات هالة في وسائل التواصل الاجتماعي عن الغذاء الصحي: «بدلاً من نشر النصائح الغذائية، اهتمي عزيزتي هالة بصحتك واعترفي أنك مصابة بمرض فقدان الشهية وأنت أصبحت كالهيكال العظمي».
	استدعت إدارة المدرسة الطالب محمد للتحقيق معه بخصوص نشره لمجموعة صور مسيئة وتعليقات نابية على معلميه وزملائه في حسابه الإلكتروني في أحد وسائل التواصل الاجتماعي، تفاجأ محمد بذلك؛ لأنه لم يكتب ولم ينشر مثل هذه المنشورات.
	عندما تصفح سامي التيك توك تفاجأ باستلام رسالة تهديد على الرسائل الخاصة من حساب مجهول ونصها: «أنا أراقبك وأعرف كل شيء عنك وستندم على قبول الدور في المسرحية». يدخل سامي على حسابه في السناپ شات ليجد رسالة تهديد أخرى «أعرف أين تسكن وأعرف كل شيء عنك».
	نشرت سارة على أحد وسائل التواصل الاجتماعي مقطعاً من مشاركتها في مسابقة الخطابة والتي حصلت فيها على المركز الثاني، ثم علّق مجهول بشكل ساخر على المقطع، حزنت سارة جداً عند قراءة التعليق وقامت بحذف المنشور.
	أرسل خالد عدداً من الاستفسارات على إحدى ساحات النقاش الطلابية، ولاحظ أن الأعضاء يتفاعلون مع كل الرسائل باستثناء رسائله، وقد تكرر هذا التصرف كثيراً.



هـ. ل. فتاة تبلغ من العمر 13 عاماً وكانت تعاني من مرض الصرع؛ في أحد الأيام الدراسية، أصيبت الفتاة بنوبة صرع وبدأ الطلاب بالتنمر عليها في المدرسة أولاً ثم انتقل التنمر إلكترونياً عبر الضحك والتلفظ عليها بألفاظ نابية. أصبحت هـ. ل. أكثر عزلة وتعاني من الاكتئاب الحاد وترفض الذهاب للمدرسة، ومع ذلك لم يتوقف التنمر الإلكتروني الذي تتعرض له من زملاء في المدرسة، وفي أحد الأيام أرسل إليها أحد الزملاء بريداً صوتياً يخبرها به أن تموت للتخلص من مرضها، وللأسف لم تعد الفتاة تتحمل المزيد من التنمر وأقدمت على الانتحار.

المصدر: صحيفة Daily mail الإلكترونية

استخرج من القصة الآثار التي عانت منها الفتاة بسبب التعرض للتنمر الإلكتروني.

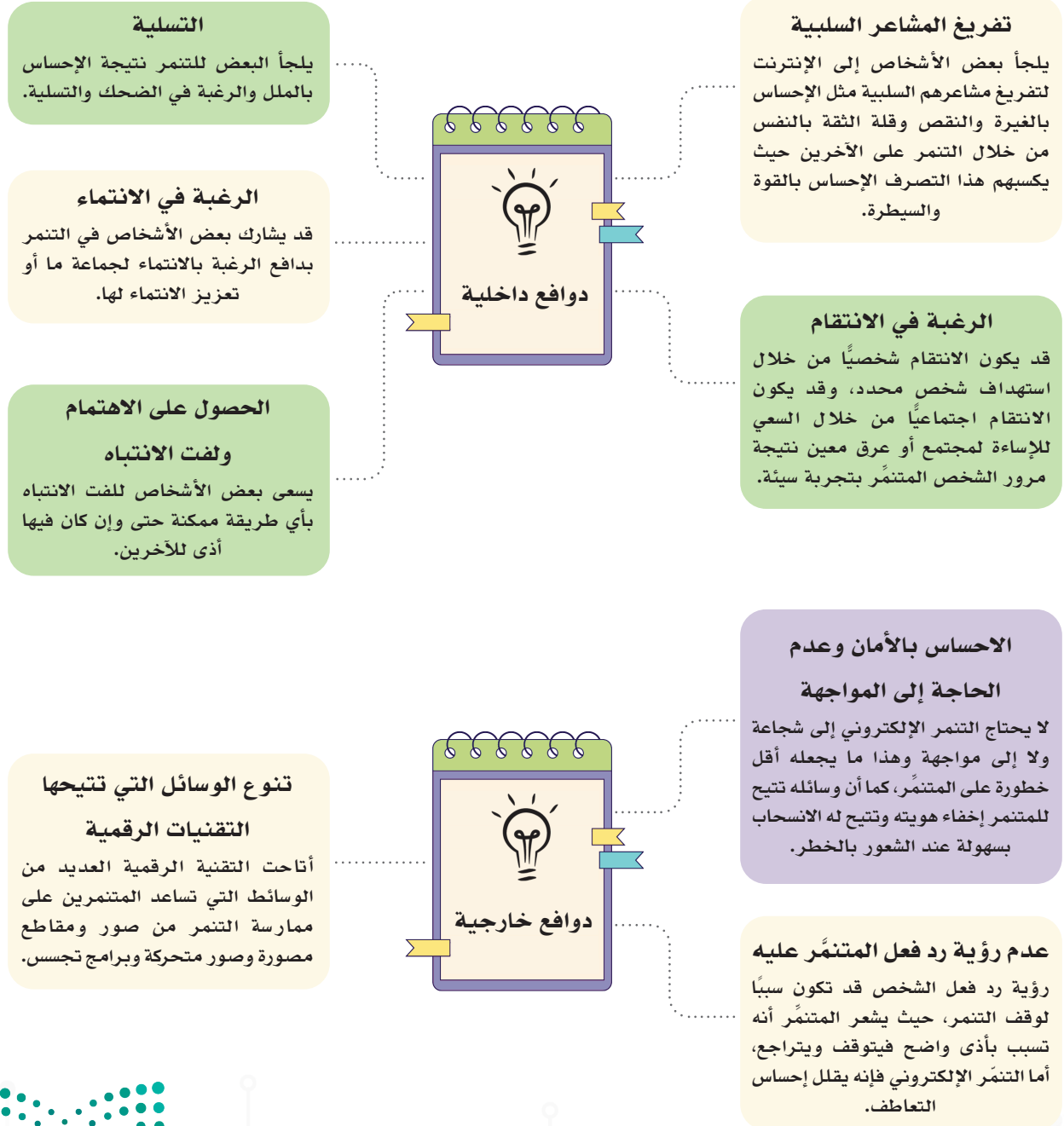
تتنوع الآثار التي يسببها التنمر الإلكتروني على الأشخاص، ويمكن تصنيفها إلى آثار نفسية وسلوكية وأكاديمية، ومنها ما هو موضح في الشكل (20-2):

آثار أكاديمية	آثار سلوكية	آثار نفسية
- عدم الرغبة في الذهاب إلى المدرسة - تدني الدرجات - فقدان الشغف بالدراسة - الغياب المتكرر عن المدرسة - ترك المدرسة	- التوقف عن استخدام الأجهزة الإلكترونية - تغير في عادات الأكل أو النوم - عدم الرغبة في المشاركة بالأنشطة الاجتماعية - العزلة الاجتماعية عن العائلة والأصدقاء - أذى النفس ومحاولة الانتحار - السلوك العدواني	- الشعور بالتوتر والقلق طوال الوقت - الشعور بالاكتئاب - الإصابة بالتقلبات المزاجية - الشعور بالخجل والانسحاب - الشعور بالغضب - التفكير بالانتحار - قلة الثقة بالنفس - الشعور بالخوف - نوبات هلع

شكل (20-2): آثار التنمر الإلكتروني

دوافع التنمر الإلكتروني

تختلف الأسباب والدوافع لحدوث التنمر الإلكتروني من شخص لآخر، ويمكن تصنيف دوافع التنمر الإلكتروني إلى دوافع داخلية وخارجية كما في الشكل (2-21).



شكل (2-21): الدوافع الداخلية والخارجية للتنمر الإلكتروني

إثارة التفكير:



كيف يمكن أن يساعد الوعي بدوافع الشخص المتنمر على التعامل مع التنمر الإلكتروني؟

كيفية التعامل مع التنمر الإلكتروني وجهود المملكة العربية السعودية لمكافحته

أولت المملكة العربية السعودية اهتمامًا خاصًا لجعل العالم الرقمي أكثر أمانًا، ومن جهودها في هذا الصدد مكافحة جرائم المعلوماتية بجميع أشكالها؛ ونظرًا للأضرار والآثار التي يسببها التنمر الإلكتروني وبسبب انتشاره على نطاق واسع أصبح يصنف كأحد الجرائم المعلوماتية، وقد سعت المملكة ممثلة ببعض الجهات الحكومية إلى التوعية بأشكال وأضرار التنمر الإلكتروني، وكيفية التعامل معه، وسن القوانين الرادعة لجميع أشكاله، وتتراوح العقوبات ما بين السجن والغرامات المالية (سيتم التطرق إلى المزيد من التفاصيل حول الجرائم المعلوماتية في الوحدة الثالثة)، وللتعامل مع التنمر الإلكتروني اتبع الخطوات الآتية :

التعامل مع التنمر الإلكتروني

في الغالب يكون هدف المتنمر هو استفزاز الهدف والحصول على ردة فعل، أو لفت الانتباه، أو التسلية وتجاهل المنشور المسيء يساعد في ردع وإيقاف المتنمر.

عدم الرد

أحد دوافع المتنمرين الرغبة في السيطرة على المتنمر عليه والشعور بالقوة والسلطة، عدم التنازل أمام المتنمر وعدم إظهار الضعف والخوف يساعد في الحد من التنمر.

عدم التنازل للمتنمر

جمع ماثبت التعرض للتنمر، عن طريق حفظ صور للقطات الشاشة وحفظ جميع الرسائل والوسائط المستخدمة من قبل المتنمر حيث يساعد ذلك في الإبلاغ عن المتنمر.

جمع الأدلة

يعتبر حظر المتنمر أحد أفضل الإستراتيجيات لوقف الأذى الحاصل منه والحد من التنمر.

حظر المتنمر

من الجيد اللجوء لشخص ثقة قد يكون أحد الوالدين أو الأخوة أو الاخصائي الاجتماعي في المدرسة وإطلاعهم على الأدلة التي توضح ما تم التعرض له من تنمر وطلب المساعدة.

طلب المساعدة

في حالة تكرار التنمر أو في حالات المطاردة والتهديد لابد من ردع المتنمر عن طريق إبلاغ الجهات المختصة بمكافحة الجرائم المعلوماتية انظر الشكل (2-22).

الإبلاغ





شكل (22-2): كيفية رفع بلاغات الجرائم المعلوماتية

إثراء

«علم واستريح» هي أحد المبادرات تحت مظلة «العطاء الرقمي» والتي أطلقتها وزارة الاتصالات وتقنية المعلومات في المملكة العربية السعودية و تهدف للتوعية بالتنمر الإلكتروني وسبل الوقاية منه، للاطلاع أكثر زر الموقع عبر مسح رمز الاستجابة السريع.

خطاب الكراهية عبر الإنترنت

أصبحت وسائل التواصل الاجتماعي وسيلة يستغلها البعض لنشر خطاب العنصرية والكراهية، وبث الفرقة بين الأفراد والمجتمعات مما تسبب بالكثير من الأضرار النفسية، والفرقة والانقسام كما أن بعض هذه الخطابات قد تحوّل إلى أعمال عنف على أرض الواقع، ويشير خطاب الكراهية عبر الإنترنت (Online hate speech) إلى هجوم يحدث عبر شبكة الإنترنت يُستخدم فيه التصريح أو التلميح بعبارات ورموز عنصرية أو تحقيره لشخص أو أشخاص بسبب انتمائهم لمجموعة معينة، فقد يكون التمييز بسبب الانتماء: لعرق، أو جنس، أو دين، أو لون، أو توجه أو أحد العوامل الأخرى المحددة للهوية.

القصة الآتية توضح أحد أشكال خطاب الكراهية عبر الإنترنت وتداعياته، اقرأ ثم أجب عن الأسئلة:

أعلن لاعب المنتخب الفرنسي السابق ت. هـ. (من أصول أفريقية) عن إغلاق حساباته في وسائل التواصل الاجتماعي احتجاجاً على العنصرية والكراهية التي يتعرض لها هو وغيره من اللاعبين عبر هذه المنصات، حيث عبر قائلًا: (اعتباراً من صباح الغد، سأقوم بتعطيل حساباتي، من السهل للغاية إنشاء حساب واستخدامه في العنصرية والمضايقة بدون أي عواقب ويظل مرتكب هذه الأفعال مجهول الهوية، وحتى يتغير هذا سأقوم بتعطيل حساباتي عبر وسائل التواصل الاجتماعي)، ثم أضاف قائلًا: (إن الحجم الهائل للعنصرية والعنف وما ينتج عنها من تعذيب نفسي للأفراد يخلق مناخاً ساماً للغاية، بحيث لا يمكن تجاهله، يجب أن يكون هناك بعض المساءلة).

المصدر: الموقع الإلكتروني لقناة العربية، 2021

استنتج من القصة:

1. الدوافع التي أدت إلى بث خطاب الكراهية.

2. دور وسائل التواصل الاجتماعي في تصعيد خطاب الكراهية.

3. الآثار المترتبة على نشر خطاب الكراهية على الإنترنت.

دور شبكة الإنترنت ووسائل التواصل الاجتماعي في تصعيد خطاب الكراهية

على الرغم من أن هذا النوع من الخطاب موجود قبل الإنترنت، إلا أن شبكة الإنترنت ومنصات التواصل الاجتماعي قد زادت من تفاقم هذه المشكلة وذلك للأسباب الموضحة في الشكل (2-23):



● صعوبة إزالة المواد من شبكة الإنترنت حيث يبقى أثر البصمة الرقمية للكثير من هذه الخطابات.

● سرعة نشر خطابات الكراهية والتي تؤدي إلى زيادة التحريض والعنصرية والتعصب.

● جمع مؤيدين وأنصار من مختلف أقطار العالم.

● سهولة نشر الشائعات والمعلومات المغلوطة عن جماعة ما.

● إمكانية إخفاء الهوية مما يعطي أمان أعلى للمشاركة في مثل هذه الخطابات.

● قلة الرقابة على شبكة الإنترنت.

● الكثرة الهائلة للمعلومات والأخبار تجعل من الصعب في بعض الأحيان تمييز الصحيح من المزيف.

● إتاحة العديد من الأدوات التي يمكن أن تساعد في انتشار خطاب الكراهية بشكل أسرع إضافة إلى أنها وسيلة جذب للمتابعين، مثل إمكانية التعليق، مشاركة المنشور، البث المباشر الصوتي والمصور.

شكل (23-2): دور وسائل التواصل الاجتماعي في تصعيد خطاب الكراهية

يرتبط خطاب الكراهية مع حرية التعبير عن الرأي وتعتبر وسائل التواصل الاجتماعي منبراً عاماً للجميع للتعبير عن آرائهم والمشاركة من خلال الكتابة أو النقر على زر الإعجاب أو إعادة مشاركة المنشور. إن حرية الرأي والتعبير حق أساسي من حقوق الإنسان على النحو المنصوص عليه في المادة 19 من الإعلان العالمي لحقوق الإنسان بحسب منظمة الأمم المتحدة وهي أيضاً حرية مكفولة بنظام الحكم السعودي، ولكن في نطاق الأحكام الشرعية والنظامية «بمعنى أن الحرية تلازمها دائماً مسؤولية»، (بالإمكان الرجوع للوحدة الأولى والاطلاع على نظام المطبوعات والنشر في المملكة العربية السعودية).



إضاءة

مستويات خطاب الكراهية عبر الإنترنت

تتفاوت مستويات خطاب الكراهية في مدى الأثر والأذى الذي تسببه، فمن خلال استخدام شبكة الإنترنت ووسائل التواصل الاجتماعي يمكن للأشخاص بث خطاب الكراهية في ثلاث مستويات يوضحها الجدول (2-4).



وزارة التعليم

Ministry of Education

2023 - 1445

جدول (2-4): مستويات خطاب الكراهية عبر الإنترنت

المستوى المنخفض	المستوى المتوسط	المستوى المرتفع
• بناء صورة سلبية عن جماعة معينة من خلال نشر أفكار وقصص وصور ومقاطع ساخرة وطُرف بشأن عدم كفاءة أو ملائمة هذه الجماعة (الجماعة قد تنتمي إلى جنس أو دولة أو مذهب أو عمل معين). • تصريحات وتعليقات بشأن عيوب أخلاقية لجماعة ما. • المساهمة في نشر بعض الاقتباسات التي تهين جماعة معينة دون التعليق عليها.	• الدفاع والتبرير عن عمل عنف قديم أو حديث وقع ضد جماعة ما. • نشر أفكار مغلوطة لتفوق عرق أو جماعة ما والتقليل من شأن جماعة أخرى. • نشر الشائعات عن التأثير السلبي على المجتمع بسبب إقامة جماعة ما فيه.	• دعوة الآخرين وتحريضهم للعنف ضد جماعة ما. • الدعوة الصريحة للتمييز العنصري. • الدعوة لنقل العنف من العالم الافتراضي للواقعي. • الدعوة والتحريض لعدم قبول السلام. • تصوير أعمال عنف ضد جماعة ما ونشرها عبر الإنترنت والحث على القيام بمثلها.

أعلنت الأمم المتحدة يوم 18 يونيو من كل عام يوماً دولياً لمكافحة خطاب الكراهية، والذي تم الاحتفال به لأول مرة عام 2022م حيث تسعى الجمعية العامة للأمم المتحدة من خلال الاحتفال بهذا اليوم إلى زيادة الوعي وتبسيط الضوء على المخاوف العالمية بشأن الانتشار المتسارع لخطاب الكراهية في جميع أنحاء العالم، واعتمدت قراراً بشأن تعزيز الحوار بين الأديان والثقافات والتسامح في مواجهة خطاب الكراهية.



طرق عملية للتعامل مع خطاب الكراهية عبر الإنترنت

هناك عدة طرق للتعامل مع خطاب الكراهية عبر الإنترنت يوضحها شكل (2-24):

حظر الحساب حظر الأشخاص المشاركين في خطاب الكراهية يظهر الرفض للعنصرية وإثارة الفتنة وخطوة لإظهار الموقف الإيجابي الراض لمثل هذه التصرفات.	عدم المشاركة بعد إعادة التوجيه والنشر أو الإعجاب بمنتشور يحتوي على خطاب كراهية أمراً خاطئاً وحثاً يوقع من يقوم بذلك بمشاكل قانونية.
--	--

الإبلاغ

يُنتهك خطاب الكراهية شروط خدمة معظم مزودي خدمات وسائل التواصل الاجتماعي فيمكن الإبلاغ عن الحساب لإدارة المنصة، كما أن خطاب الكراهية يندرج ضمن جرائم المعلوماتية ويمكن الإبلاغ عن أي حساب يروج للفكر العنصري من خلال تطبيق «كلنا أمن».

زيادة الوعي

أحد الأسباب الرئيسية في انتشار خطاب الكراهية هو الجهل بحقيقة الآخر وتداعيات هذا النوع من الخطاب على الأفراد والمجتمعات، التثقيف حول أشكال خطاب الكراهية وتداعياته قد يساعد في الحد منه.

تعزيز القيم

من خلال المساهمة في نشر وتعزيز قيم التسامح، والعدالة، والمساواة، والتعاطف.

شكل (24-2): التعامل مع خطاب الكراهية عبر الإنترنت

أ | جهود المملكة العربية السعودية في الحد من خطاب الكراهية عبر الإنترنت

تم التوضيح سابقاً (الوحدة الأولى) القوانين التشريعية التي أقرتها المملكة العربية السعودية لنظام المطبوعات والنشر والتي أسهمت بشكل كبير في تجريم خطاب الكراهية والحد منه، ولكن جهود المملكة لم تتوقف عند ذلك، حيث إن جهودها سعت إلى مكافحة خطاب الكراهية من خلال منظومة علاجية متكاملة تشمل الجوانب المعرفية والقيمية والسلوكية والقانونية، هذا بالإضافة للتعاون الدولي لتحقيق الهدف المنشود، اقرأ النص الآتي للتعرف أكثر على جهود المملكة في هذا المجال:

رسخت المملكة العربية السعودية ثقافة التسامح وتعزيز قيمه ونبذ صور وملامح التطرف والكراهية والعنف؛ إيماناً منها بأن التسامح بين الناس أساس للتعايش، ومنهج حياة، ومن المبادئ الجامعة بين الأفراد، وبناء الحضارات، وتنتظر المملكة للقيم الإسلامية السمحة كنهج لتعزيز الأمن والاستقرار والتسامح بين كل المجتمعات الإنسانية بمختلف جنسياتهم وانتماؤاتهم السياسية والثقافية ليكونوا نسيجاً واحداً ضد كل ما يهدد تلاحمهم وتماسكهم، حيث كان لمركز الملك عبدالعزيز للحوار الوطني دور رئيس في تعزيز هذه المفاهيم وترسيخها وجعلها جزءاً أصيلاً من ثقافة المجتمع، كما قام مركز الملك عبدالله بن عبدالعزيز العالمي للحوار بين أتباع الأديان والثقافات، ببذل الجهود الكبيرة نحو تعزيز ثقافة الحوار وترسيخ التعايش واحترام التنوع وقبول التعددية ودعم المواطنة المشتركة بين الدول، وقد أنشأت المملكة المركز العالمي لمكافحة الفكر المتطرف «اعتدال»، الذي يعمل على تحجيم خطاب الكراهية ومحاصرة دعائه من خلال تجفيف منابع الكراهية في وسائل الإعلام والشبكات الاجتماعية التي كانت سبباً في تشكيل بيئة خصبة لترويج ونشر هذا الخطاب من قبل الجماعات المتطرفة، وتشجيع الناس للإبلاغ عن جرائم الكراهية، وتعزيز دور التربية والتعليم تجاه مكافحة خطاب الكراهية ودعم ثقافة التعايش الإنساني، وإطلاق مبادرات أخلاقية تحفز على نبذ الكراهية ونشر قيم الاعتدال.

المصدر: وكالة الأنباء السعودية (واس)، 2022 (بمصرف)

1. في النص السابق، أكدت حكومة المملكة العربية السعودية على أهمية تعزيز قيم التسامح والاعتدال والمساواة لمكافحة خطاب الكراهية وهي قيم مستقاة من الشريعة الإسلامية السمحة، باستخدام شبكة الإنترنت، ابحث عن المقصود بكل من:

● التسامح:

● الاعتدال:

● المساواة:

2. لماذا تعد هذه القيم أساسية لمكافحة خطاب الكراهية عبر الإنترنت؟

.....

3. من خلال تصميم رسم معلوماتي (Infographic)، وضح الجهود التي أولتها حكومة المملكة العربية السعودية لمكافحة خطاب الكراهية. (بالإمكان تصميمه في المساحة أدناه أو تصميمه إلكترونياً).

4. في النص السابق تؤكد المملكة على دور التعليم الإيجابي تجاه مكافحة خطاب الكراهية ودعم ثقافة التعايش الإنساني. اقترح حلولاً تساعد في تفعيل دور التعليم في نبذ خطاب الكراهية عبر الإنترنت.

.....

.....

.....

.....



مما درست، ما الفرق بين مفهوم كل من الدراما الرقمية والتنمر الإلكتروني وخطابات الكراهية عبر الإنترنت؟

الخطاب الكراهية عبر الإنترنت	التنمر الإلكتروني	الدراما الرقمية

غذاء الفكر



- تفكّر في أشكال أخرى للعنف الإلكتروني غير المذكورة في الدرس.
- لماذا تكثر الدراما الرقمية في أوساط المراهقين؟
- ما الفئات الأكثر عرضة لمشاكل التنمر الإلكتروني؟ وكيف يمكن حمايتهم؟
- البوت (Bot) هو أحد التقنيات التي يتم استخدامها في تصعيد خطاب الكراهية، ما هو؟ وكيف يتم تفعيله؟

نقاط مهمة

- تكثر الدراما الرقمية في أوساط المراهقين والشباب، انتبه من أن تكون أحد المشاركين في تصعيدها أو أحد ضحاياها.
- في حالة تعرضك للتنمر الإلكتروني، تذكر أنك لست الملام وأن التنمر الإلكتروني غالبًا ما يكون بسبب دوافع داخلية نفسية تتعلق بالشخص المتنمر، حاول أن تفصل تمامًا بين نظرتك إلى نفسك وبين ما يقوله عنك المتنمرون.
- قال ﷺ: (انْصُرْ أَخَاكَ ظَالِمًا أَوْ مَظْلُومًا، قالوا: يَا رَسُولَ اللَّهِ، هَذَا نَنْصُرُهُ مَظْلُومًا، فَكَيْفَ نَنْصُرُهُ ظَالِمًا؟ قَالَ: تَأْخُذُ فَوْقَ يَدَيْهِ) [صحيح البخاري، 2444] الموقف الإيجابي لوقف العنف الإلكتروني فيه نصرة للشخص المستهدف وتنبيه المتنمر لوقف أذاه.



مشروع الدرس



يتضح من خلال الدرس الدور الأساسي الذي تقوم به التوعية تجاه مكافحة كافة أشكال العنف الإلكتروني. بالتعاون مع زملائك صمم ملصقًا تعليميًا (poster) يهدف إلى التوعية المجتمعية بأشكال العنف الإلكتروني من خلال:

اقتراحات للعمل:

- بإمكان كل مجموعة اختيار شكل من أشكال العنف الإلكتروني (الدراما الرقمية - التنمر الإلكتروني - خطاب الكراهية عبر الإنترنت) لعمل الملصق التعليمي.
- توضيح كل من:
 - المفهوم.
 - الأسباب.
 - كيفية التعامل معه.
 - سبل الحماية منه.
- يمكن أن يتم تصميم الملصق إلكترونيًا أو باستخدام لوح ورقي.
- عرض الملصق على المعلم والزملاء في الفصل ثم عرضه في المدرسة عبر لوحة الإعلانات.





الصحة والالتزان في العالم الرقمي

مخرجات التعلم:

- أتعرف على مفهوم الإدمان الرقمي.
- أميز الأعراض التي تدل على حالة الإدمان الرقمي.
- أحلل الأسباب التي قد تؤدي إلى الإدمان الرقمي.
- أوضح العلاقة بين الإدمان الرقمي وإدمان المخدرات.
- أتعرف على مفهوم الاتزان الرقمي.
- أفرق بين الاستخدام المتزن والإدمان الرقمي.
- أناقش التأثير الإيجابي والسلبي للتقنية الرقمية على الصحة.
- استخدم التطبيقات التي تساعد في المحافظة على الصحة.
- أطبق بعض الطرق لتحقيق الاتزان الرقمي.
- أتعرف على جهود المملكة العربية السعودية في تحقيق الاتزان الرقمي.
- أساهم في التوعية بأخطار الإدمان الرقمي وأهمية الاتزان الرقمي.



مصطلحات الدرس:

- الإدمان الرقمي (Digital Addiction)
- الصحة الرقمية والاتزان الرقمي (Digital Health and Digital Wellbeing)
- اضطراب الألعاب عبر الإنترنت (Internet gaming disorder)

التهيئة

أصبحت الأجهزة الإلكترونية والتطبيقات والخدمات الرقمية ذات صلة وثيقة بحياتنا اليومية، فبالرغم من الفوائد الجمة التي أحدثتها التقنية الرقمية في حياة الإنسان، إلا أن الإفراط في استخدامها يؤثر سلباً على مختلف جوانب الحياة حتى أصبحت التقنية الرقمية عوناً وعبئاً في الوقت نفسه، وفي هذا السياق، يجب التعامل مع مسألة الإدمان الرقمي وتأثيره على الصحة، والوعي بكيفية تحقيق الاتزان الرقمي بمزيد من الجدية من خلال تبني نهج متوازن وواعٍ حول الاستخدام السليم لوسائل التقنية الرقمية، وطرح الأسئلة الآتية:

- هل التقنية الرقمية عدو أم صديق؟
- هل تشعر بالقلق عند عدم تمكنك من الاتصال بالإنترنت؟
- عند قضاء الوقت مع الأهل والأصدقاء، هل يشغلك الهاتف المحمول عن الحديث معهم؟
- كيف أصبح البعض منا من مدمني الإنترنت؟
- هل سبق لك أن استخدمت أحد التطبيقات الرقمية للمحافظة على الصحة؟



الإدمان الرقمي

يشير الإدمان الرقمي (Digital Addiction) إلى اضطراب التحكم في الانفعالات بسبب الاستخدام المفرط للأجهزة الإلكترونية والإنترنت والألعاب الإلكترونية ومنصات التواصل الاجتماعي.



يعد مفهوم الإدمان الرقمي مجال ناشئ ضمن علم النفس السيبراني (Cyberpsychology) لذلك لا توجد معايير تشخيصية حتى الآن للإدمان الرقمي، ولكن في الإصدار الحادي عشر من التصنيف الدولي للأمراض الصادر من منظمة الصحة العالمية تم إدراج اضطراب الألعاب عبر الإنترنت (Internet gaming disorder) كنوع من سلوكيات الإدمان الرقمي التي تستدعي التدخل الطبي.

نشاط



24-2

قيم علاقتك بالتقنية الرقمية من خلال الإجابة على الاستبيان.

ملاحظة: إذا انطبقت عليك 5 أو أكثر من العبارات الآتية فهي مؤشر على فرط الاستخدام.

لا ينطبق	ينطبق لحد ما	ينطبق	مؤشرات الإدمان الرقمي
			1. أقضي أغلب وقت فراغي في استخدام الهاتف الذكي وتصفح الإنترنت.
			2. أشعر بعدم الراحة عند نسيان هاتفي أو إذا لم يكن قريباً مني.
			3. أستخدم الهاتف الذكي وقت المذاكرة وأداء الواجبات.
			4. أستخدم الهاتف الذكي أثناء جلوسي مع الأهل والأصدقاء.
			5. أفتح الهاتف الذكي وأتحقق من التنبيهات مرة واحدة على الأقل كل 30 دقيقة.
			6. أمضي الكثير من الوقت في تصفح حساباتي في وسائل التواصل الاجتماعي قبل النوم.
			7. أمسك بهاتفي الذكي لحظة استيقاظي من النوم.
			8. استمر في لعب بعض الألعاب الإلكترونية بشكل متواصل لأكثر من ساعتين.



يوجد العديد من الاختبارات للتحقق من مدى التعلق بالأجهزة والمنصات الرقمية، بإمكانك القيام بعمل اختبار من خلال مسح رمز الاستجابة السريع، وهو اختبار من إعداد «سينك» برنامج الاتزان الرقمي التابع لمركز الملك عبد العزيز الثقافي العالمي.

نوموفوبيا (Nomophobia): رهاب فقدان الهاتف الذكي وهي اختصار (no-mobile-phone phobia)، هي الشعور بالخوف من فقدان الهاتف الذكي، أو ضعف بطاريته، أو التواجد خارج نطاق تغطية الشبكة، حيث يُصبح الشخص مضطرباً وقلقاً جداً فتتسارع نبضات قلبه وضغط دمه، ويضيق نفسه، وقد يشعر بالهلع في الحالات الشديدة.

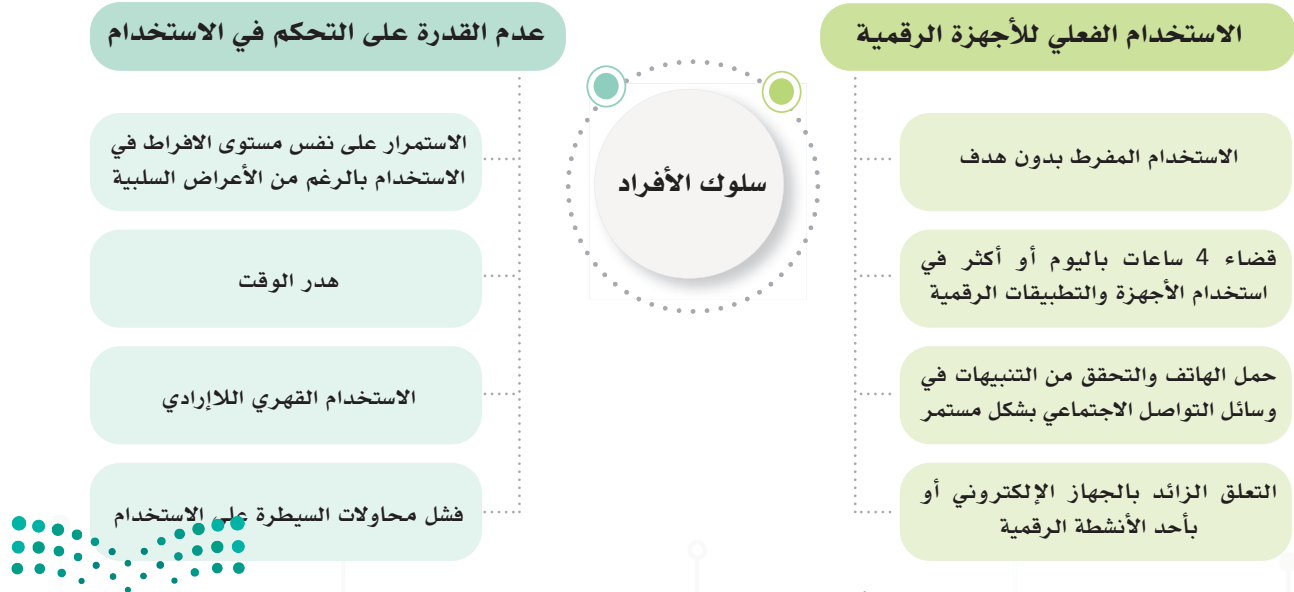


المصدر: المعهد الوطني للصحة The National Institutes of Health (NIH) التابع لوزارة الصحة الأمريكية

أعراض الإدمان الرقمي

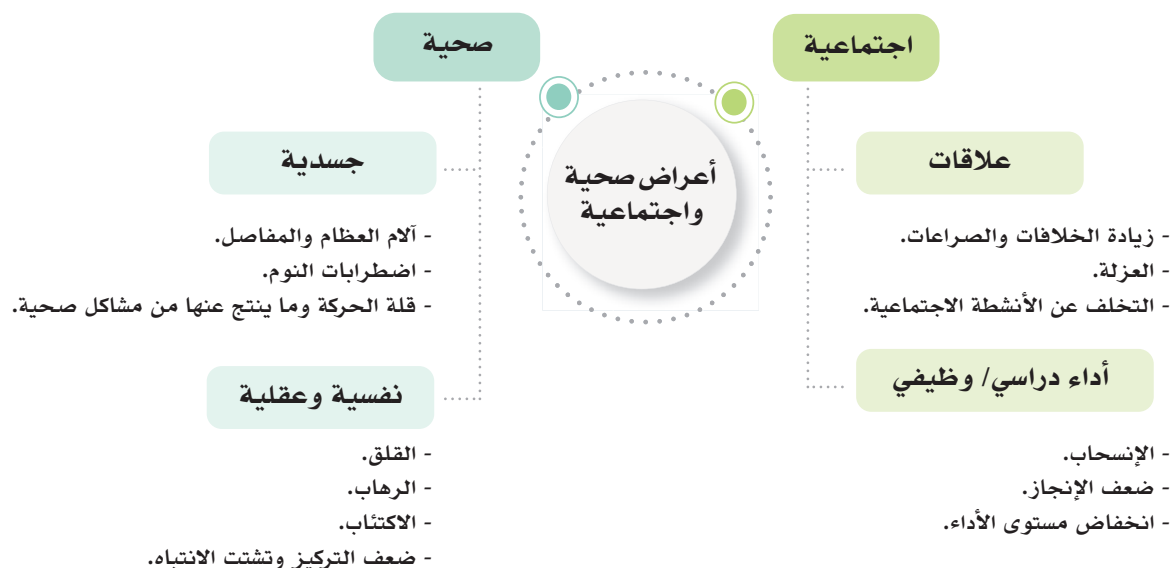
تمت الإشارة سابقاً إلى أن الإدمان الرقمي لم يصنف حتى الآن كمرض، وبالتالي لا يوجد تشخيص محدد للكشف عنه، ومع ذلك هناك أعراض يمكن أن تساعد الأفراد أو الوالدين أو المختصين في تمييز الإدمان الرقمي، وتصنف هذه الأعراض إلى:

1. أعراض سلوكية: يوضح الشكل (2-25) بعض الأعراض السلوكية التي تظهر على الأفراد وتشير إلى وجود إدمان رقمي، من حيث الإفراط في الاستخدام، وعدم القدرة على التحكم في استخدام الأجهزة الرقمية.



شكل (25-2): الأعراض السلوكية التي تشير إلى حالة الإدمان الرقمي

2. أعراض صحية واجتماعية: يوضح الشكل (2-26) الأعراض الصحية التي يسببها الإدمان الرقمي على الصحة الجسدية والعقلية والنفسية للأفراد والأعراض الاجتماعية من حيث تأثيره على العلاقات والأداء الدراسي أو الوظيفي



شكل (2-26): الأعراض الصحية والاجتماعية التي تشير إلى حالة الإدمان الرقمي

أسباب الإدمان الرقمي

هناك العديد من الأسباب التي أدت إلى شيوع الإدمان الرقمي، منها:

1. عوامل اجتماعية: تؤدي بعض حالات عدم الاستقرار الأسري ومشاكل العلاقات إلى الهروب من الواقع عبر الإدمان الرقمي.
2. أسباب نفسية: الشعور بالاكتئاب والقلق والرهاب الاجتماعي قد تكون عوامل مؤدية إلى الإدمان الرقمي، حيث يساعد الوجود في العالم الرقمي المستخدم في الإحساس بالانتماء والسعادة.
3. إدمان الدوبامين (Dopamine): التواجد الرقمي يساعد على إفراز هرمون الدوبامين والذي يعطي المستخدم إحساس بالسعادة وهذا يجعله يميل للإفراط في الاستخدام للحصول على المزيد من نفس الشعور.
4. طريقة تصميم التقنية الرقمية: يسعى المختصون في تصميم التقنية الرقمية إلى جذب انتباه المستخدم وضمان بقاءه من خلال إعطاء المستخدم تجربة متجددة دون الانتباه إلى السلوك القهري الذي يدفعه للاستخدام المفرط للأجهزة والمنصات الرقمية.



يوضح الشكل (27-2) بعض الطرق التي يستخدمها المختصون في تصميم التقنية الرقمية والتي يمكن أن تزيد من حالة الإدمان الرقمي.

طرق جذب انتباه المستخدم

التصميم

نظام المكافآت حيث يساعد على رفع هرمون الدوبامين من خلال تقنيات مثل: الإعجاب، التعليق، المشاركة، معرفة عدد المتابعين ومن شاهد المنشور) أو الانتقال من مستوى لآخر في الألعاب أو الحصول على نقاط.

الانتقال التلقائي: يحرص مصممو الألعاب ومنصات التواصل على بقاء المستخدم لأطول فترة ممكنة من خلال الانتقال التلقائي للمقطع التالي أو المرحلة التالية.

التحديث المستمر: إمكانية سحب الشاشة لأسفل للحصول على المزيد من الأخبار والمنشورات مما يضمن بقاء المستخدم لفترة طويلة.

استخدام الألوان التي تجذب انتباه وتركيز المستخدم.

الخوارزميات: من خلال جمع بيانات المستخدم من أجل

استهداف المستخدم بالإعلانات مما قد يؤدي إلى النهم الشرائي.

تخصيص تجربة المستخدم حسب تفضيله وميوله لضمان بقاءه.

شكل (27-2): طرق تصميم التقنية الرقمية المسببة للإدمان الرقمي

إثارة التفكير:



ما الذي يجب على المختصين في تصميم التقنية الرقمية عمله للتخفيف من ظاهرة الإدمان الرقمي؟



العلاقة بين الإدمان الرقمي وإدمان المخدرات

كما تم التوضيح سابقاً، يؤدي الإدمان الرقمي إلى مشاكل في الصحة العقلية والنفسية والعلاقات الاجتماعية، وهذه الأعراض قد تدفع المدمنين الرقميين إلى الهروب من المشاكل التي يعانون منها إلى مشكلة أكبر وهي إدمان المواد المخدرة، فهناك علاقة بين إدمان المخدرات والإدمان الرقمي حيث إن:

1. الإدمان الرقمي قد يؤدي إلى إدمان المخدرات والعكس صحيح أي أن إدمان المخدرات قد يكون أحد الأسباب للإدمان الرقمي.
2. علاج حالات إدمان المخدرات لا بد وأن يتزامن مع علاج الإدمان الرقمي إن وجد وإلا فإن الشخص يصبح أكثر عرضة للانتكاس.
3. الأعراض السلوكية والصحية والاجتماعية التي تظهر على المدمن الرقمي مشابهة لأعراض إدمان المخدرات.

نشاط مجتمعي



1. بعد دراسة أعراض الإدمان الرقمي، ابحث عبر شبكة الإنترنت عن أعراض إدمان المخدرات واستنتج أوجه الشبه بين الإدمان الرقمي وإدمان المخدرات من حيث تأثيرهما على الصحة العقلية والنفسية والعلاقات الاجتماعية.
2. من خلال الرسم المعلوماتي (Infographic)، وضح العلاقة بين الإدمان الرقمي وإدمان المخدرات وأوجه الشبه بينهما.
3. شارك الرسم المعلوماتي مع معلمك وزملائك في الفصل.
4. انشر الرسم المعلوماتي على أحد وسائل التواصل الاجتماعي كنوع من التوعية المجتمعية.

تعتبر مهارة إدارة الوقت من أهم مهارات القرن 21 ولأهمية الوقت فهو مما يسأل عنها العبد يوم القيامة، فعن أبي بركة الأسلمي رضي الله عنه قال، قال رسول الله ﷺ: (لا تزول قدما عبد يوم القيامة حتى يسأل عن عمره فيما أفناه، وعن علمه فيم فعل، وعن ماله من أين اكتسبه وفيم أنفق، وعن جسمه فيم أبلاه) [صحيح الترمذي، 2417]؛ فأحسن استثمار وقتك.



إضاءة



تأمل ذاتي:

1. لمدة 24 ساعة، تتبّع نشاطك الرقمي:

النشاط الرقمي		وصف تفصيلي للنشاط الرقمي
الوقت الإجمالي لاستخدام الهاتف الذكي خلال 24 ساعة		
عدد المرات التي قمت بحمل وفتح الهاتف الذكي		
تسجيل النشاط الرقمي (سجل تكرار السلوك)	مراسلة	
	لعب	
	متابعة وسائل التواصل الاجتماعي	
	قراءة أخبار	
	أخرى (أذكرها بالتفصيل)	
الحالة الشعورية بعد قضاء فترة في استخدام تطبيقات الهاتف الذكي		
مدة استخدام الهاتف الذكي قبل النوم		
استخدام الهاتف الذكي عند الاستيقاظ من النوم		

2. بناء على المعلومات التي حصلت عليها، قيم ممارساتك الرقمية.

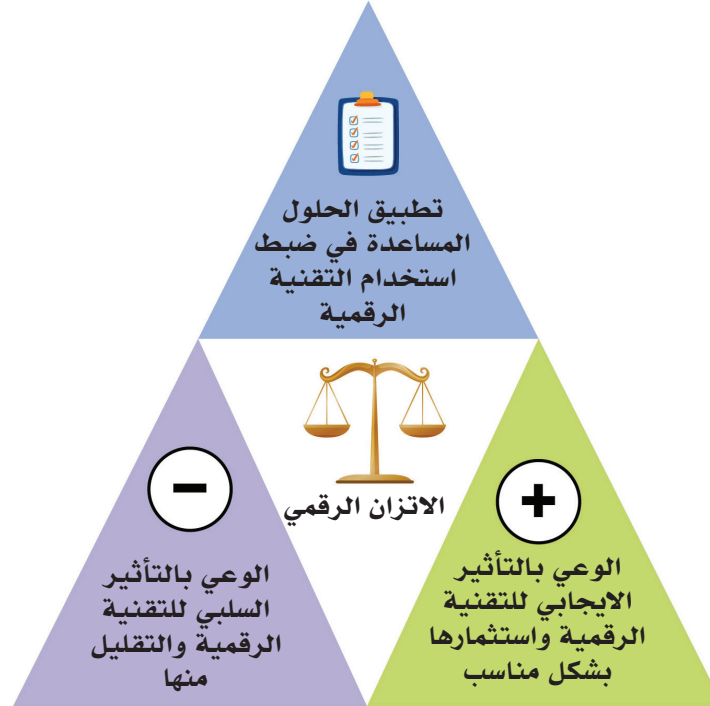
أ. هل يعتبر استخدامك مفرطاً؟ وضع إجابتك.



ب. ما هي النشاطات الرقمية التي تستهلك وقتك؟ وما مدى تأثيرها عليك؟

الصحة والاتزان الرقمي

يعد الاتزان الرقمي من الحلول الناجحة لمواجهة خطر الإدمان وتشير الصحة والاتزان الرقمي (Digital Health and Wellbeing) إلى الوصول لحياة متزنة صحية يستطيع فيها الأفراد التحكم في استخدام التقنية الرقمية واستثمار الوقت، حيث يكمن التوازن عبر الاستفادة من إيجابيات التقنية الرقمية مع الحد من أضرارها المحتملة. يُظهر الشكل (28-2) ثلاثة جوانب أساسية لا بد من الوعي بها سعياً لتحقيق الاتزان الرقمي وهي:



شكل (28-2): العوامل المساعدة على تحقيق الاتزان الرقمي

|| التأثير الايجابي والسلبي للتقنية الرقمية على الصحة

الوعي بالآثار الإيجابية والسلبية للتقنية الرقمية يساعد في الوصول لحالة الاتزان الرقمي حيث يمكن أن تؤثر التقنية والأنشطة الرقمية على الصحة الجسدية والنفسية للأفراد، والعلاقات الاجتماعية، والقدرة على التعلم، والبيئة، والعمل وغيره من السياقات بطرق إيجابية وسلبية، ويوضح الشكل (29-2) تأثير التقنية الرقمية على الصحة.

تأثير التقنية على صحة الأفراد

— التأثير السلبي

- أضرار على الصحة الجسدية (مثل إجهاد العين، أوجاع العنق والظهر والمعصم، مشاكل في السمع، اضطرابات النوم، قلة النشاط البدني مما يسبب أمراض كالسمنة، والقلب، والسكري، والتهاب المفاصل).
- أضرار على الصحة النفسية (مثل القلق، الاكتئاب، نوبات الغضب والخوف، قلة الانتباه، تشتت التركيز، الشعور بالوحدة، قلة الثقة بالنفس، وغيرها من المشاكل النفسية).

+ التأثير الإيجابي

- متابعة حالة الصحة الجسدية من خلال التطبيقات، والأجهزة القابلة للارتداء والتي تساعد في تتبع النشاط البدني، مراقبة الوزن، وضربات القلب، اتباع حمية غذائية، ضبط ساعات النوم.
- إتاحة العديد من التطبيقات التي تساعد على تحسين الصحة النفسية مثل تطبيقات الاسترخاء، وتبني الحالة المزاجية.
- تطبيقات ومواقع تساعد في التشخيص الذاتي المبكر لبعض الأمراض الجسدية والنفسية.

شكل (29-2): التأثير الايجابي والسلبي للتقنية الرقمية على صحة الأفراد



إثراء



يوفر موقع وزارة الصحة حزمة من الأدوات الصحية الرقمية التي تساعد على تحسين الصحة الجسدية والنفسية والتشخيص الذاتي المبكر لبعض الأمراض، للاطلاع امسح رمز الاستجابة السريع.

نشاط



ارسم صورة تعبيرية توضح الآثار الإيجابية والسلبية للتقنية الرقمية على الصحة.

--	--

نشاط



1. ابحث عن تطبيق من التطبيقات الخاصة بتحسين الصحة الجسدية أو النفسية.
2. استخدم التطبيق لمدة أسبوع.
3. اكتب تقريراً يوضح: اسم التطبيق، آلية عمله، تقييمك للتطبيق، إلى أي مدى ساعد في رفع الوعي وتحسين الحالة الصحية.
4. شارك تجربتك حول هذا التطبيق في صفحتك على أحد وسائل التواصل الاجتماعي.



طرائق عملية مساعدة في تحقيق الاتزان الرقمي

يعرض الشكل (2-30) مجموعة من الطرائق والحلول المساعدة على تحقيق الاتزان الرقمي، منها:

إلغاء التنبيهات.
ضبط المدة التي يتم فيها استخدام الجهاز.
ضبط خلفية الجهاز على اللون الرمادي لتقليل الرغبة في الاستخدام.
الاكتفاء بالبرامج الأساسية على الصفحة الرئيسية لشاشة الهاتف الذكي (Home Screen) لتقليل الاستخدام.
عدم استخدام الهاتف المحمول أو أي جهاز إلكتروني قبل النوم.
ضبط الجهاز على وضع عدم الإزعاج عند الانخراط في عمل ما.
الحرص على القيام بأنشطة مختلفة لا تتطلب استخدام الأجهزة الرقمية (مثل: القراءة، الرياضة، نزهة خارجية).
التوقف عن استخدام الأجهزة الرقمية أو بعض وسائل التواصل الاجتماعي لفترة بسيطة من الزمن.

شكل (2-30): طرائق تحقيق الاتزان الرقمي



جهود المملكة العربية السعودية في تحقيق الاتزان الرقمي



ضمن سعي المملكة العربية السعودية لتحقيق حياة أفضل، تم إطلاق «برنامج الاتزان الرقمي (سينك)» وهو أحد مبادرات مركز الملك عبد العزيز الثقافي العالمي «إثراء» وتتمثل رؤية البرنامج في إيجاد عالم متزن لمستخدم التقنية الرقمية. حيث تعنى المبادرة برفع الوعي من خلال دعم البرامج والمؤتمرات العلمية الحوارية والأبحاث والشراكات لدراسة تأثير التقنية على حياتنا سعيًا لتطوير ممارسات رقمية سليمة وتحقيق الاتزان في عصر التحول الرقمي، بالإمكان الاطلاع على المبادرة من خلال مسح رمز الاستجابة السريع.

إثراء



يقدم مركز الملك عبد العزيز الثقافي العالمي "إثراء" العديد من البرامج والخبرات في مختلف المجالات الثقافية ومن ضمنها مجال التقنية الرقمية، بإمكانك الاطلاع على مبادرة إثراء والاستفادة من البرامج المقدمة من خلال مسح رمز الاستجابة.

بطاقة المواطن الرقمي

بعد الانتهاء من تعلّم بعض الطرائق لتحقيق الاتزان الرقمي، أكمل الجدول لتوضيح ما تم تحقيقه:

م	الطريقة المتبعة لتحقيق الاتزان الرقمي	تاريخ التنفيذ
1		
2		
3		
4		
5	اقترح طرقًا مبتكرة يمكن من خلالها تحقيق الاتزان الرقمي: 1. 2. 3. 4.	



أجرى مركز «إثراء» دراسة عالمية لرصد تأثير التقنية الرقمية على حياة الجمهور العالمي، ونُشر التقرير الخاص بنتائج الدراسة عام 2022م، امسح رمز الاستجابة للاطلاع على التقرير، ومن ثم أجب عن الأسئلة الآتية:

1. ما هو تصنيف المملكة العربية السعودية بين دول العالم في مؤشر الاعتماد على الوسائل الرقمية؟ ما رأيك بهذه النتيجة؟

2. توضح النتائج أن 48% من مستخدمي الإنترنت يقضون وقتاً أطول مما خططوا له في التصفح. بحسب رأيك، ما الأسباب المؤدية إلى هذه النتيجة؟

3. أظهرت الدراسة أن 53% من الناس يفضل العيش بدون صديق مقرب على فقد هاتفه الذكي، ما رأيك بهذه النتيجة؟ وما أسبابها وكيف يمكن علاجها؟

4. ما تداعيات استخدام التقنية الرقمية على الصحة؟



اختر إحدى الصور الآتية وعبر عنها من خلال:

1. وصف شعورك بعد تأمل الصورة.
2. تفسير الرسالة الرئيسية التي تحاول الصورة التعبير عنها.
3. اقتراح حلول تساعد الشخصية الظاهرة في الصورة على تحقيق الاتزان الرقمي.



صورة 2



صورة 1

اكتب إجابتك هنا:

غذاء الفكر



- قام بعض المختصين المساهمين في تطوير خدمات شبكات التواصل الاجتماعي في كل من «فيسبوك» و «جوجل» و «انستغرام» بالتوعية من أخطار ما صنعوه، تأمل لماذا يطلق أصحاب التقنية هذا التحذير وهم من صنعها؟!
- راقب التأثير الذي يتركه صوت التنبيه أو ظهور إشعار باستلام رسالة عبر هاتفك الذكي على سلوكك، ما رأيك؟
- عند خروجك لمكان عام، استقطع بضع دقائق من وقتك لتتأمل حال من حولك مع هواتفهم الذكية، هل يعجبك ما ترى؟

نقاط مهمة

- قال تعالى: ﴿وَلَا تُلْقُوا بِأَيْدِيكُمْ إِلَى التَّهْلُكَةِ وَأَحْسِنُوا إِنَّ اللَّهَ يُحِبُّ الْمُحْسِنِينَ﴾ [البقرة: 195]، الاستخدام المتوازن والمسؤول يقي بإذن الله من المشاكل التي قد يسببها استخدام التقنية الرقمية.
- ضبط النفس وتحقيق الاتزان الرقمي يحتاج إلى تدريب وممارسة وصبر.
- دورك كمواطن رقمي مهم جداً بنشر المعرفة والوعي بأضرار الإدمان الرقمي.

مشروع الدرس



بالتعاون مع زملائك، صمم مقطعاً مرئياً (Video) توعوياً يوضح المقصود بالإدمان الرقمي وأضراره وأعراضه وأسبابه، مع توضيح بعض الحلول لتحقيق الاتزان الرقمي، ثم ارفع الفيديو التعليمي على أحد وسائل التواصل الاجتماعي وشارك الرابط مع المعلم وبقية الزملاء.

1. تقسيم العمل بين أعضاء الفريق:

الوقت المتوقع للإنجاز	المهمة	الاسم

2. كتابة السيناريو الخاص بالمقطع المرئي:

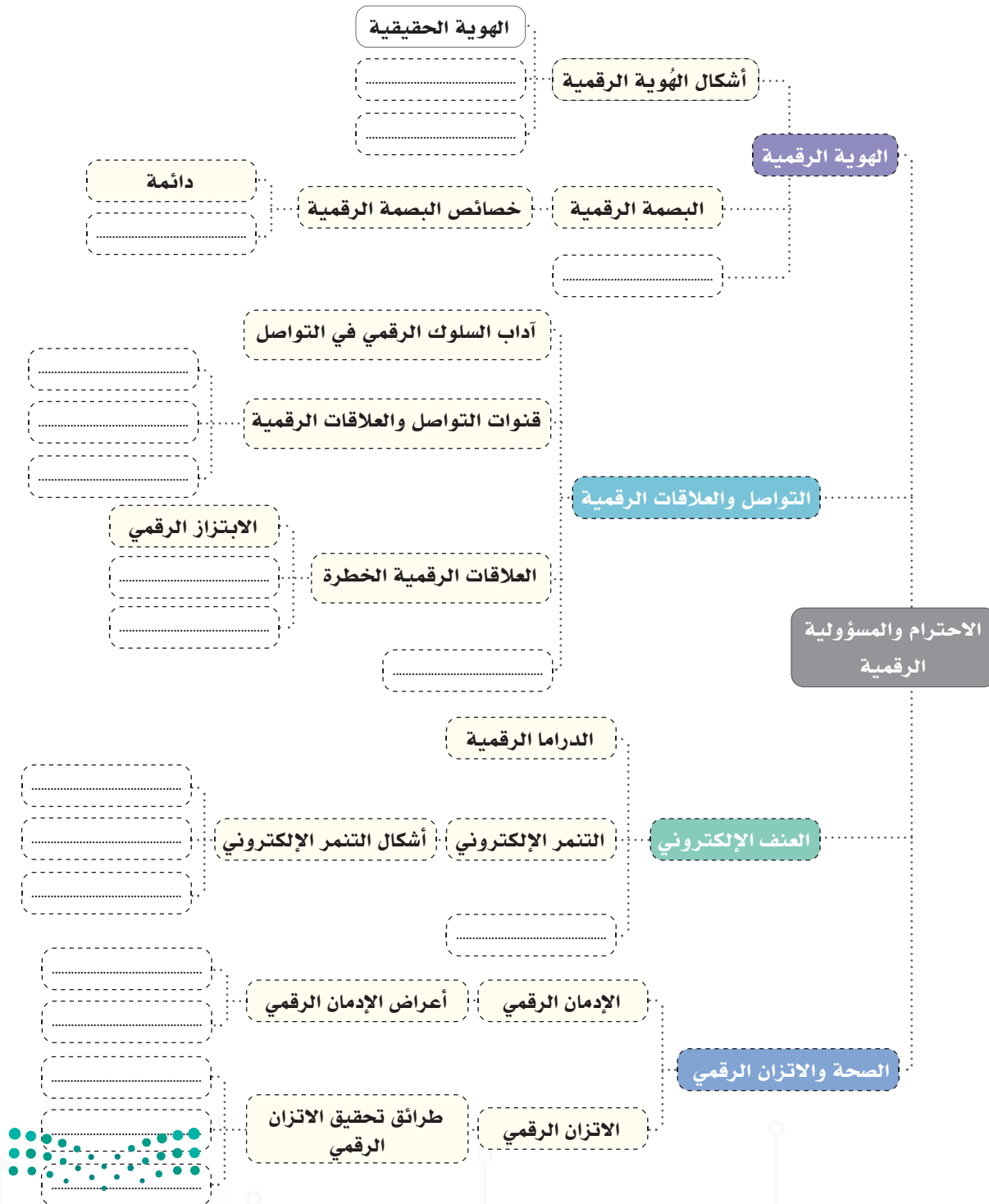
3. الاتفاق على البرنامج المستخدم لتنفيذ المقطع المرئي:

4. المنصة التي سيتم رفع المقطع المرئي التوعوي عليها:



خريطة مفاهيم الوحدة

أكمل الخريطة المفاهيمية الآتية:



تقويم الوحدة

السؤال الأول: ضع إشارة (✓) أمام العبارة الصحيحة وإشارة (X) أمام العبارة الخطأ:

الإجابة	العبارة
	1. يمكن إزالة البصمة الرقمية للمستخدمين بسهولة.
	2. تعد تقنية الواقع المعزز إحدى قنوات التواصل والعلاقات الرقمية.
	3. من آثار الدراما الرقمية أنها قد تؤدي إلى فقدان الثقة وقطع العلاقات.
	4. تعد مهارة تبديل نمط اللغة إحدى مهارات التواصل للحد من التنمر الإلكتروني.
	5. من الأساليب المستخدمة في بناء الهوية الرقمية المأمولة ادعاء امتلاك بعض المهارات أو المبالغة في تعظيم الإنجازات البسيطة.
	6. الدفاع والتبرير عن عمل عنف حصل ضد جماعة ما يصنف كمستوى منخفض في خطاب الكراهية عبر الإنترنت.
	7. تعتبر الإساءة غير المتعمدة أحد أشكال التنمر الإلكتروني.
	8. يعد التعاطف مهارة مهمة في آداب السلوك الرقمي كونها تساعد في تعزيز السلوك الإيجابي.
	9. يصنف اضطراب الألعاب عبر الإنترنت كمرض يستدعي التدخل الطبي.
	10. يشير السلوك العدواني أو الانطوائي إلى احتمالية تعرض الشخص لتنمر إلكتروني.
	11. الإدمان الرقمي مشكلة سلوكية يمكن الاستدلال عليها بفرط الاستخدام.
	12. يعتبر تقبل النقد من مهارات المشاركة في الحوار الرقمي المتحضر.
	13. تكمن أهمية الاتزان الرقمي في التحكم بالاستخدام من خلال الاستفادة من إيجابيات التقنية الرقمية مع الحد من أضرارها المحتملة.
	14. الدافع الأساسي لخطابات الكراهية عبر الإنترنت هو الاختلاف في العرق فقط.



السؤال الثاني: اختر الإجابة الصحيحة في كل مما يأتي:

الخيارات	الجملة
أ. الابتزاز الرقمي.	1. تخويف الشخص أو تهديده بكشف معلومات خاصة أو محرجة عنه ونشرها عبر شبكة الإنترنت بهدف التحكم به للقيام بأعمال غير قانونية، أو للحصول على المال. يعد تعريفا لمفهوم:
ب. الضغط.	
ج. السيطرة.	
أ. الهوية الرقمية.	2. الصورة الذهنية التي يبنها المتابع - أو ما يفكر به الناس ويعتقدونه - عن مستخدم الإنترنت ووسائل التواصل الاجتماعي. هي تعريف لمفهوم:
ب. البصمة الرقمية.	
ج. السمعة الرقمية.	
أ. تشويه سمعة.	3. يعتبر التجاهل المتعمد لرسالة شخص ضمن مجموعة في أحد وسائل التواصل الاجتماعي، أحد أشكال:
ب. الإقصاء.	
ج. الخداع.	
أ. الإفراط في استخدام الأجهزة التقنية.	4. يمكن تمييز الإدمان الرقمي من خلال:
ب. التشخيص الطبي.	
ج. شراء جهاز إلكتروني جديد.	



الجملة	الخيارات
5. من مهارات إدارة البصمة الرقمية:	أ. المشاركة بشكل مستمر لإثبات الوجود الرقمي
	ب. التحقق من المعلومات قبل النشر
	ج. السبق في نشر كل جديد
6. تتميز العلاقات الرقمية الصحية ب:	أ. الاحترام المتبادل
	ب. التواصل اليومي
	ج. التعليق على كل منشور يشاركه الصديق
7. هدف المتصيد Troll في التنمر الإلكتروني هو:	أ. التسلية
	ب. الانتقام
	ج. زيادة عدد المتابعين



أقيّم ما تعلّمت في الوحدة

بناءً على ما تعلّمت من دروس في هذه الوحدة؛ قيّم نفسك ذاتياً عبر معايير التقييم الموضحة في الجدول، واحسب مجموع النقاط المكتسبة.

● 2 = ينطبق بدرجة عالية.

● 1 = ينطبق بدرجة متوسطة.

● 0 = لا ينطبق.

النقاط المكتسبة	مقاييس التقدير			معيّار التقييم
	0	1	2	
2/.....	لم أعرف مفهوم الهوية الرقمية، والبصمة الرقمية، والسمعة.	عرّفت مفهوم الهوية الرقمية، والبصمة الرقمية، والسمعة الرقمية بشكل صحيح بنسبة (50%)	عرّفت مفهوم الهوية الرقمية، والبصمة الرقمية، والسمعة الرقمية بشكل صحيح بنسبة (100%)	1. تعريف مفهوم الهوية الرقمية، والبصمة الرقمية، والسمعة الرقمية.
2/.....	لم أعدد خصائص البصمة الرقمية.	عددت (1) إلى (2) من خصائص البصمة الرقمية.	عددت (3) إلى (5) من خصائص البصمة الرقمية.	2. تعداد خصائص البصمة الرقمية.
2/.....	لم أطبق طرق إدارة البصمة الرقمية، والسمعة الرقمية.	طبقت (2) إلى (3) من طرق إدارة البصمة الرقمية، والسمعة الرقمية.	طبقت (4) إلى (6) من طرق إدارة البصمة الرقمية، والسمعة الرقمية.	3. تطبيق مهارات إدارة البصمة الرقمية، والسمعة الرقمية.
2/.....	لم أطبق آداب وأخلاقيات المواطن الرقمية الصالحة.	طبقت (2) إلى (4) من آداب وأخلاقيات المواطن الرقمية الصالحة.	طبقت (5) إلى (7) من آداب وأخلاقيات المواطن الرقمية الصالحة.	4. تطبيق آداب وأخلاقيات المواطن الرقمية الصالحة.
2/.....	لم أفرق بين أنواع العلاقات الرقمية.	أفرق إلى حد ما بين العلاقات الرقمية الصحية وغير الصحية والعلاقات الرقمية الخطرة.	أفرق بين العلاقات الرقمية الصحية وغير الصحية والعلاقات الرقمية الخطرة بدرجة كبيرة جداً.	5. التفريق بين العلاقات الرقمية الصحية وغير الصحية والعلاقات الرقمية الخطرة.
2/.....	لم أطبق طرق ضبط حدود التواصل والعلاقات الرقمية.	طبقت (4) إلى (6) من طرق ضبط حدود التواصل والعلاقات الرقمية.	طبقت (7) إلى (10) من طرق ضبط حدود التواصل والعلاقات الرقمية.	6. وضع حدود صحية للعلاقات الرقمية.
2/.....	لم أطبق إستراتيجيات المشاركة في حوار رقمي متحضر.	طبقت إستراتيجيات المشاركة في حوار رقمي متحضر بشكل صحيح بنسبة (70%).	طبقت إستراتيجيات المشاركة في حوار رقمي متحضر بشكل صحيح بنسبة (100%).	7. المشاركة في حوار متحضر عبر شبكة الإنترنت.

أقيّم ما تعلّمت في الوحدة

النقاط المكتسبة	مقاييس التقدير			معيّار التقييم
	0	1	2	
2/.....	لم أُميّز بين أشكال العنف الإلكتروني وطرق التعامل معها.	أُميّز أشكال العنف الإلكتروني بشكل صحيح بنسبة (70%)، وأذكر اثنين من الطرق الفعالة للتعامل مع كل نوع.	أُميّز أشكال العنف الإلكتروني بشكل صحيح بنسبة (100%)، وأذكر أربعة من الطرق الفعالة للتعامل مع كل نوع.	8. تمييز أشكال العنف الإلكتروني والطرق الفعالة للتعامل معها.
2/.....	تصنيفي لأنواع التنمر الإلكتروني غير صحيح، أو لم أطبق النشاط.	تصنيفي لأنواع التنمر الإلكتروني صحيح بنسبة (70%).	تصنيفي لأنواع التنمر الإلكتروني صحيح بنسبة (100%).	9. تصنيف أنواع التنمر الإلكتروني الشائعة.
2/.....	لم أقترح حلول عملية تساعد في تفعيل دور التعليم في مكافحة خطاب الكراهية عبر الإنترنت، أو لم أطبق النشاط.	اقترحت من (1) إلى (2) حلول عملية تساعد في تفعيل دور التعليم في مكافحة خطاب الكراهية عبر الإنترنت.	اقترحت من (3) إلى (5) حلول عملية تساعد في تفعيل دور التعليم في مكافحة خطاب الكراهية عبر الإنترنت.	10. اقتراح حلولاً تساعد في تفعيل دور التعليم في مكافحة خطاب الكراهية عبر الإنترنت.
2/.....	لا أعرف مفهوم الإدمان الرقمي ولا أذكر أعراضه.	أعرف مفهوم الإدمان الرقمي بشكل صحيح بنسبة (70%)، وأذكر (1) إلى (2) من أعراضه.	أعرف مفهوم الإدمان الرقمي بشكل صحيح بنسبة (100%)، وأذكر (3) إلى (5) من أعراضه.	11. تعريف مفهوم الإدمان الرقمي وذكر أعراضه.
2/.....	لم أستخدم أحد التطبيقات الرقمية لتحسين الصحة، ولم أعد تقريراً.	أستخدم أحد التطبيقات الرقمية لتحسين الصحة، ولا أعد تقريراً عن تجربتي.	أستخدم أحد التطبيقات الرقمية لتحسين الصحة، وأعد تقريراً عن تجربتي.	12. استخدام التطبيقات الرقمية لتحسين الصحة.
2/.....	لم أطبق إستراتيجيات الوصول للتوازن الرقمي.	طبقت (1) إلى (2) من إستراتيجيات الوصول للتوازن الرقمي.	طبقت (3) إلى (5) من إستراتيجيات الوصول للتوازن الرقمي.	13. تطبيق الطرق المساعدة في الوصول للتوازن الرقمي.
26/.....	المجموع			

لحساب مجموع النقاط:

- 20 فأعلى = متمكن بدرجة عالية.
- من 14 إلى 19 = متمكن إلى حدٍ ما.
- أقل من 14 = غير متمكن.





الوحدة الثالثة



وزارة التعليم

Ministry of Education

2023 - 1445

الأمان والحماية الرقمية

Digital Safety and Security

تسلط هذه الوحدة الضوء على القسم الأخير لمقرر المواطنة الرقمية (الأمان والحماية الرقمية)، وتقدم الوحدة نبذة عن الكيفية التي يكون المواطن الرقمي واعياً لممارساته الرقمية للحماية من الجرائم السيبرانية، ومتمكناً بوسائل الحماية من التهديدات الرقمية التي يواجهها في العالم الرقمي، وفهم القوانين والأنظمة التي تنظم التعامل بين الأفراد مع بعضهم البعض، وبين الأفراد والجهات الحكومية والتجارية، وكيفية مساهمة المواطن الرقمي في توعية الآخرين للعيش في عالم آمن.

متطلبات الوحدة

تحتوي بعض الدروس على تطبيقات عملية تحتاج إلى توفير جهاز حاسوب، خدمة إنترنت، نظامي تشغيل الويندوز والهواتف الذكية، برمجيات مساعدة، تطبيقات الهواتف الذكية.



أهداف التعلم

بنهاية هذه الوحدة سيكون الطالب قادراً على:

1. استيعاب مفهوم الجرائم السيبرانية، ودوافعها، وتصنيفاتها وطرائق الإبلاغ عنها حال وقوعها.
2. التعرف على قوانين مكافحة الجرائم السيبرانية، والتوعية حول أضرار الجرائم السيبرانية، وعقوبات ارتكابها.
3. استيعاب خطر التهديدات الرقمية، وتطبيق الممارسات الآمنة لتجنبها ذاتياً وبرمجياً.
4. استشعار أهمية الحفاظ على المعلومات للمواطن الرقمي.
5. تنمية الوعي بطرائق التعامل مع التهديدات الرقمية في شبكة الإنترنت.
6. استيعاب مفاهيم الخصوصية وأهمية حمايتها، وتطبيق ممارسات الحماية الآمنة لها.
7. تقديم التوعية للمجتمع بأهمية الحفاظ على الخصوصية وأمان المعلومات.
8. استيعاب مفاهيم الملكية الفكرية، والتمييز بين أنواع الحقوق الفكرية، وقواعد الاستلham من أعمال الآخرين.
9. استشعار أهمية الملكية الفكرية على المجتمع وآثارها، ونشر التوعية عن أهميتها.
10. تثمين جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية، وحماية حقوق الملكية الفكرية.





الجرائم السيبرانية

وجهود مكافحتها محلياً ودولياً

الدرس الأول

مخرجات التعلم:



- أتعرف على الجريمة السيبرانية، وأركانها، والفرق بين مصطلحاتها.
- أشارك في وضع حلول لعوائق مكافحة الجرائم السيبرانية.
- أناقش دوافع ارتكاب الجريمة السيبرانية، وآثارها على الحكومات والشركات.
- أصنف الجرائم السيبرانية الشائعة عبر شبكة الإنترنت.
- أبلغ عن الجريمة السيبرانية حال وقوعها.
- أتعرف على أهمية الجهود العربية والعالمية في مكافحة الجرائم السيبرانية.
- أؤمن 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 الفيروسات الحاسوبية المشهورة كسلامر (Slammer)، ولوف (ILOVEYOU)، وساسر (Sasser) من تعطل للأجهزة، وتشفير للملفات، ومدى تأثيرها المادي والمعنوي؟
- ماذا لو تعرض 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 بدلاً من ممارسة العمل السليم؟
- هل سمعت عن خبر لمخالفة معلوماتية في إحدى وسائل الإعلام الرقمية؟ وما رأيك في تصرف صاحبها؟
- هل تفكر قبل إجراء أي عمل أثناء استخدامك شبكة الإنترنت ما إذا كان نافعاً أم ضاراً لك أو لغيرك؟
- هل تشعر بالندم لتصرف مارسته سابقاً أثناء استخدامك لشبكة الإنترنت؟ وكيف تداركت الموقف في وقتها؟

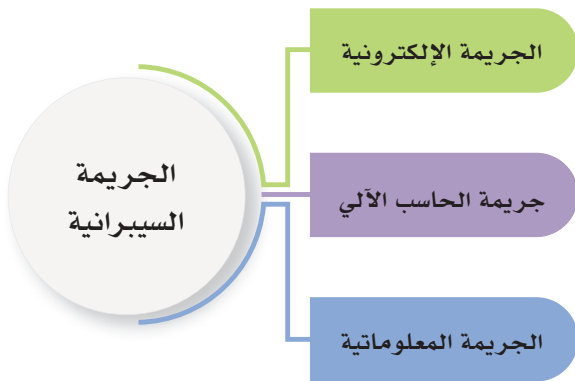
|| الجريمة السيبرانية والمصطلحات المرتبطة بها

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 (1-3)، إلا أن أكثرها تداولاً في المنظمات الدولية هي الجريمة السيبرانية (CyberCrime) التي تعرف بأنها: (نشاط إجرامي يستهدف أو يستخدم جهاز حاسوب أو شبكة حاسوبية أو جهازاً متصلاً 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 (1-3): مصطلحات الجرائم السيبرانية

يتوافق مفهوم (الجريمة السيبرانية) كثيراً مع مصطلحات (الجريمة الإلكترونية)، (الجريمة المعلوماتية)، (جريمة



شكل (2-3): توافق مصطلحات الجرائم السيبرانية

الحاسب الآلي) كونها جميعاً تعبر 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 ثمَّ يُعد متقارباً مع المصطلحات الأخرى في حال كون الموضوع يتعلق بالاعتداءات التي تكون ضمن محيط الحاسوب سواء كانت مادية أو معنوية.

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:

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

النوع الثاني

المخترقون (الهكرز Hackers)، وهم مجموعة من الأشخاص متخصصون في الاختراق، ويتواصلون مع بعضهم افتراضياً من دول مختلفة لتبادل الخبرات، والتعاون فيما بينهم لتنفيذ ممارساتهم إما لأهداف سياسية أو عسكرية بالإضافة للانتفاع المالي الذي يعد الهدف الأساسي.

النوع الأول

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.

ثانياً: 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.

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

نشاط فردي



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



أنشطة الجرائم السيبرانية

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

جدول (1-3): أنشطة الجرائم السيبرانية

1	التزوير باستخدام الحاسوب.	2	الاختيال 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 كالكذب 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 شرعياً 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.

إثارة التفكير:



هل يمكنك إضافة أنشطة أخرى غير المذكورة في الأعلى؟



بناء على اطلاعك على قائمة الأنشطة الإجرامية في جدول (1-3)، صنف الممارسات 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 للمشاركين.	
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.	



يُبين 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 تعلم 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	التفريد عبر تطبيق تويتر عن أخبار غير صحيحة.		

أ| عوائق مكافحة الجريمة السيبرانية:

توجد عدة عوائق يصعب معها مكافحة الجريمة السيبرانية، ويجب دراسة هذه العوائق لمحاولة فهمها، وتحليل أسباب وجودها؛ للتقليل منها قدر المستطاع ومحاولة القضاء عليها، ومن هذه العوائق انظر الشكل (3-3):



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، خصوصاً 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 مرتكبها.

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



اقترح حلولاً لعوائق مكافحة الجرائم السيبرانية التي درستها.

مهن وتخصصات الأمن السيبراني: ظهرت عدة مهن وتخصصات في مجال الأمن السيبراني، منها:

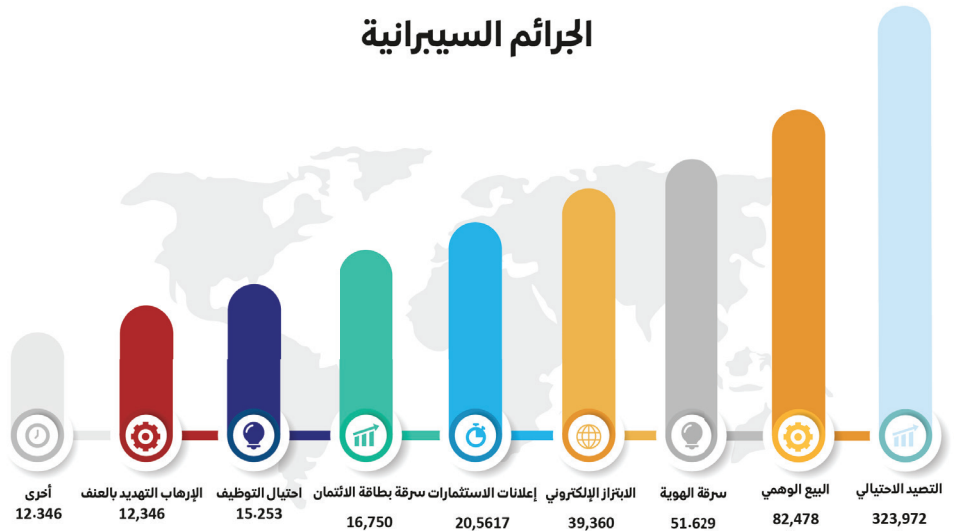
- محلل أمن سيبراني.
- أخصائي أمن سيبراني.
- محلل جنائي رقمي.
- مدير شبكة أمن معلومات.
- أخصائي دفاع أمن سيبراني.
- مطور برامج شبكية.



إضاءة

الجرائم السيبرانية الأكثر انتشاراً على مستوى دول العالم

الجرائم السيبرانية



شكل (4-3): إحصائية أنشطة الجرائم السيبرانية بحسب أعداد المتضررين لعام 2022م (statista.com)

آثار الجريمة السيبرانية على الحكومات والشركات:

اقرأ القصة الآتية:

تم اختراق شركة مشهورة عالمياً 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 سابقاً من إدارة الشركة، وأظهروا الرسالة الآتية: (لقد استطعنا السيطرة على الشركة لأنها لم تغلق الأبواب جيداً، وبالتعاون مع أحد موظفي الشركة)، وبعد عدة أيام، نشر المخترقون حسابات البريد الإلكتروني للموظفين، وبعض إنتاجات الشركة التي كلفت ملايين الدولارات، بعدها توالى 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.

بناءً على ما ورد في القصة من أحداث، بيّن آثار الجريمة السيبرانية على الشركة عبر الإجابة عن الأسئلة الآتية:

1. ما دور الشركة المتوقع عندما تم إعلامها عن مطالب المخترقين السابقة وقبل إتمام عملية الاختراق؟

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

3. ناقش الأسباب التي ساعدت على إتمام عملية الاختراق.

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

5. تحدث عن فوائد هذه القصة.

تؤثر الجريمة السيبرانية بشكل مباشر وغير مباشر على الحكومات والقطاع الخاص والأفراد، في المجالات الاقتصادية، والسياسية، والاجتماعية، والشخصية أيضاً، ويعود ذلك التأثير بسبب الإصرار الدائم والمتواصل لمقتحمي الأنظمة والشبكات على إجراء عمليات الاختراق التي تؤدي إلى تعطل أو تلف الأنظمة مما يعرض الأعمال والخدمات للتوقف، وفقد البيانات، مما يكلف كثيراً من الشركات الكبيرة والمتوسطة على مستوى العالم خسائر باهظة تصل إلى مئات الملايين من الدولارات خلال فترة التوقف عن العمل التي قد تستمر لساعات عدة، كذلك يصل تأثير الجريمة السيبرانية إلى الأفراد عبر الوصول لبياناتهم الشخصية، والمهمة، واستغلالها قدر المستطاع.





بلغ عدد هجمات البرمجيات الخبيثة في النصف الأول لعام 2022م إلى 2.8 مليار هجمة، وكان نصيب هجمات برامج الفدية منها 236 مليون هجمة، نصيب الشركات منها 70% تقريباً (statista.com)، بينما تم تقدير عدد الهجمات في الربع الأخير من العام 2022م بمعدل 1168 هجمة أسبوعياً حيث زادت نسبة الهجمات مقارنة بعام 2021م بمعدل 38% (CheckPoint.com)، كما أن هناك عدداً من الشركات تخرج من سوق التجارة الإلكترونية خلال ستة أشهر من الهجوم عليها، ويرجع سبب ذلك للخسارة المالية أولاً، ومن ثمّ خسارة السمعة والثقة في المقام الثاني.

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 لاحقاً كالإمارات العربية المتحدة، والكويت، والمملكة الأردنية الهاشمية، وجمهورية مصر العربية، وغيرها من الدول. مع تسارع الدول العربية لإقرار قانونها الخاص؛ أسست جامعة الدول العربية في عام 2010م (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 بجهود في هذا الجانب كما يتضح في الشكل (3-5) الآتي:

الشرطة الدولية (Interpol)

- ملاحقة المطلوبين بين الدول، وتقديم المعلومات المشتركة للقضاء عليهم.
- تحليل الجريمة السيبرانية، وطرائق تنفيذها لمنع تكرار وقوعها في ظروف مماثلة مستقبلاً.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)

- تعاون المكتب مع الدول الأعضاء لدراسة الجريمة السيبرانية، والتصدي لها عبر تبادل التشريعات الوطنية، والمساعدة الفنية لأفضل الممارسات.

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.

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

هل تعلم أن تكلفة الجرائم السيبرانية على الدول والمنظمات تصل إلى مليارات الدولارات سنوياً ونزاد نسبته بشكل دوري، ومن المتوقع أن تصل تكلفة خروقات البيانات (Data Breaches) إلى خمس تريليونات دولار بحلول عام 2024م



جهود المملكة العربية السعودية في مكافحة الجريمة السيبرانية

اهتمت حكومة المملكة العربية السعودية بالمحافظة على الأمن السيبراني، والحماية من الجرائم السيبرانية عبر إقرارها لقانون مكافحة الجرائم المعلوماتية، حيث تولت هيئة الاتصالات وتقنية المعلومات التصدي لهذه المهمة، ثم تم إنشاء الهيئة الوطنية للأمن السيبراني في عام 1439هـ، وتُعنى هذه الهيئة بتنظيم إستراتيجية الأمن السيبراني داخل الدولة، ووضع الآليات، والأطر، والمعايير، للجهات الحكومية، وغير الحكومية المتعلقة بالأمن السيبراني، وتحديثها باستمرار، كما أنشأت الهيئة مركزاً للتوعية والتنبية بأخطار الأمن السيبراني من هجمات أو برمجيات ضارة أو اكتشاف ثغرات، وإشراك المجتمع للتعاون على مساعدتها لمواجهة هذه الأخطار.

تفوقت المملكة العربية السعودية عالمياً في مجال الأمن السيبراني عام (2021م) بحصولها على المركز الثاني ضمن المؤشر العالمي للأمن السيبراني، والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا في المؤشر العالمي للأمن السيبراني الذي تصدره وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات «الاتحاد الدولي للاتصالات»، وذلك ضمن قياس مدى التزامها بالأمن السيبراني من بين الدول العالمية.



إثراء



قم بزيارة لمركز الجرائم السيبرانية والأدلة الرقمية التابع لجامعة الأمير نايف العربية للعلوم الأمنية على شبكة الإنترنت، واستعرض الخدمات والمجهودات التي يقدمها عبر المسح على رمز الاستجابة السريع:

نشاط



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

اسم الفعالية	تاريخ الفعالية	الجهة المنظمة

طرائق الإبلاغ عن الجرائم السيبرانية بالمملكة العربية السعودية

نشاط



اكتشف 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		

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 والمقولات المفهومة لكل منها، وذلك لتحقيق الأهداف الآتية:

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.

|| بعض مواد النظام التي تظهر العقوبات

المادة الثالثة	
يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:	
1	التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح- أو التقاطه أو اعتراضه.
2	الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا.
3	الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
4	المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
5	التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

المادة الرابعة	
يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:	
1	الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
2	الوصول -دون مسوغ نظامي صحيح- إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.



المادة الخامسة	
يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:	
1	الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها.
2	إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
3	إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المادة السادسة	
يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:	
1	إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.
2	إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.
3	إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.
4	إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المادة السابعة	
يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:	
1	إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.
2	الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.



نشاط



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

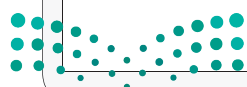
م	الممارسة الرقمية	المادة المتوافق معها	مدة عقوبة السجن	مبلغ الغرامة المالية
1	الدخول إلى البيانات الائتمانية أو البنكية دون أي تصريح قانوني.			
2	تصوير شخص يمشي في أحد شوارع مدينتك.			
3	إنشاء مواقع غير قانونية.			
4	الاطلاع على البريد الإلكتروني لأحد زملائك في المدرسة.			
5	الترويج للمواقع والحسابات 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 شخص ما وابتزازه لدفعه وإجباره على القيام بفعل معين.			

نشاط جماعي



تذكر مع مجموعتك خمس مخالفات معلوماتية وقعت في محيطك الشخصي، أو أطلعت 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.

نشاط



9-3



قم بزيارة لصفحة (البرنامج العالمي لمكافحة الجريمة السيبرانية) التابع لمكتب المخدرات والجريمة بموقع الأمم المتحدة على شبكة الإنترنت، واكتب تقريراً موجزاً عن النشاطات التي يمارسها المكتب في مكافحة الجريمة السيبرانية، وارفعها لمدونة المادة، يمكنك الوصول للصفحة عبر مسح رمز الاستجابة السريع.

نشاط



10-3

باستخدام إحدى حساباتك في وسائل التواصل الاجتماعي، انشر توعية كمواطن رقمي لبعض المخالفات المعلوماتية المنتشرة، وبين المادة المتوافقة معها في قانون مكافحة جرائم المعلوماتية السعودي.





- تأمل مع التطور السريع لخدمات الإنترنت أن يقابلها عدم وجود أمان رقمي منظم، كيف تتوقع أن تتم الإجراءات المالية والخدمات الحكومية؟ وكيف تستطيع الجهات التجارية ممارسة نشاطاتها؟.
- زيادة تخصصات الأمن السيبراني يساعد بشكل كبير في مكافحة الجرائم السيبرانية، هل تفكر في أن تكون من أحد المختصين بها؟



نقاط مهمة

- يعد تعاون المنظمات الدولية مع الشرطة الدولية (الإنتربول) في محاولة القضاء على الجريمة السيبرانية أو الحد منها تعاوناً فعالاً وإيجابياً يصب في مصلحة جميع دول العالم.
- دور كل مواطن رقمي هو تقديم المساعدة الفاعلة في التوعية عن الجرائم السيبرانية، وخطورتها التي قد تعيق تقدم الاقتصاد والإنتاج والتطور.
- لا يشترط لتكون مختصاً في الأمن السيبراني أن تكون لديك شهادة جامعية في هذا المجال، فالمجالات مفتوحة عبر الشهادات الدولية، والدورات المتعددة، والاستفادة من الخبرات المتراكمة عبر شبكة الإنترنت.



مشروع الدرس



نفذ المشروع الآتي بعد التنسيق مع معلّمك وذلك باتّباع الخطوات الآتية:

1. كوّن فريق عمل مع اثنين من زملائك في الصف الدراسي.
2. اختار إحدى الموضوعات الآتية:
 - أضرار الجريمة السيبرانية على المجتمع.
 - قصص حديثة عن أشهر الجرائم السيبرانية العالمية.
 - جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية.
3. ارجع إلى مصادر المعلومات المتعددة عبر شبكة الإنترنت: قواعد البيانات، الموسوعات، محركات البحث، مواقع الهيئات والمنظمات.
4. صمّم عرضاً مرئياً لا يقل عن سبع شرائح تشمل شريحة العنوان، شريحة المراجع.
5. ادمع العرض بالصور، والجداول، والرسومات حسب الحاجة.
6. جهّز العرض ليكون على هيئة توعية رقمية يغطي الموضوع المختار.





الحماية من التهديدات الرقمية

الدرس الثاني

مخرجات التعلم:



- أفرّق بين أمن المعلومات وأمان المعلومات.
- أستشعر أهمية المحافظة على معلوماتي من التهديدات الرقمية.
- أتعرف على التهديدات الرقمية الشائعة في شبكة الإنترنت.
- أنمي وعيي بالتعامل مع التهديدات الرقمية الشائعة في شبكة الإنترنت.
- أمارس الحماية الذاتية من التهديدات الرقمية الشائعة أثناء استخدام شبكة الإنترنت.
- أستخدم البرمجيات والتطبيقات لحماية معلوماتي على أجهزتي المتعددة.
- أقدم التوعية للمجتمع عن أهمية الحفاظ على أمان المعلومات.

مصطلحات الدرس:

- التهديدات الرقمية (Digital Threats).
- أمن المعلومات (Information Security).
- البرامج الضارة (Malware).
- أمان المعلومات (Information Safety).
- انتزاع الفدية (Ransomware).
- الابتزاز الإلكتروني (Online Blackmail).
- القرصنة الإلكترونية (Electronic Piracy).
- انتحال الهوية (Identity Theft).
- التصيد الاحتيالي (Phishing Scams).
- الهندسة الاجتماعية (Social Engineering).

التهيئة

تقدم شبكة الإنترنت خدمات رائعة للعالم أجمع، لكن كما تقدّم في الدرس السابق، لا يخلو عالم الإنترنت من الجرائم السيبرانية كاختراقات الأجهزة، والتهديدات الرقمية، مما يستدعي أن يظل الفرد واعياً بهذه التهديدات، وحريصاً على الاستمرار بالتعلّم للتصدي لها في سبيل حماية معلوماته، وممتلكاته. وأن يكون مواطناً رقمياً فاعلاً بالمساهمة بنشر التوعية والتوجيه للمجتمع الرقمي.

- هل تتحقق من اسم وعنوان الرسالة ومرسلها على بريدك الإلكتروني قبل فتحها؟
- هل تحمي حاسوبك؟ وهل تفضّصه بشكل دوري لتتأكد من خلوّه من الفيروسات؟
- كيف تتعامل مع الجهاز عندما يصاب بأحد البرامج الضارة؟
- عندما يصلك رابط عبر إحدى تطبيقات جهازك الذكي، ما الإجراءات التي تقوم بها؟
- هل تعمل نسخ احتياطي لمفاتيح المهمة باستمرار وفي مكان آمن؟
- هل تعرف أحداً تم اختراق حسابه في تطبيق الواتساب (WhatsApp)؟ إذا كانت الإجابة بـ(نعم) فكيف تعامل مع هذا الاختراق؟

أمن المعلومات (Information Security)، وأمان المعلومات (Information Safety)



تطلب بعض البرمجيات والتطبيقات من المستخدم السماح لها بمشاركة الملفات، أو تشغيل الوحدات الملحقة بالجهاز، أو قد تطلب الموافقة على مشاركة المعلومات أثناء تثبيتها. يمكن للمستخدم من العمل على هذه التطبيقات، ومن ثمّ سيكون هناك من يشارك المستخدم بالاطلاع على معلوماته المحفوظة في جهازه، بسبب أن أنظمة التشغيل قد تتعرض للمراقبة أو الاختراق المباشر أو التجسس، ولهذا ينبغي على المواطن الرقمي حماية

معلوماته الشخصية باتباع إجراءات أمن المعلومات (Information Security) وهي حماية معلوماته الخاصة من السرقة، أو الإفشاء، أو التخريب، وإدخالها في الوضع الآمن للمحافظة عليها، كما ينبغي أن يطبق المواطن الرقمي إجراءات أمان المعلومات (Information Safety) بوضع المعلومات في حالة أمان بعد حمايتها، وضمان المحافظة عليها لعدم تعرضها لأي تهديدات رقمية (Digital Threats) متوقعة في المستقبل.

نشاط



بالعودة إلى التعريفين السابقين، وضّح ما يجب عليك كمواطن رقمي التعامل معه أولاً لحماية معلوماتك الرقمية (أمن المعلومات) أم (أمان المعلومات)؟ ولماذا؟



نشاط



بالتعاون مع مجموعتك، أذكر خمسة أمثلة على معلومات رقمية مهمة يجب عليك حفظها، وحمايتها من التعرض للتلف، أو السرقة، أو الاطلاع عليها من قبل الآخرين.

1.
2.
3.
4.
5.

نشاط



بالتعاون مع أفراد مجموعتك، توقع ما يمكن أن يفعله مجرمو شبكة الإنترنت أثناء حصولهم على معلوماتك الشخصية:

1.
2.
3.
4.
5.



أنواع التهديدات الرقمية (Digital Threats) الشائعة عبر شبكة الإنترنت

الهندسة الاجتماعية Social Engineering

استدراج المستخدم للحصول منه على أي معلومات تساعد المحتالين لإجراء أعمال احتيال أو سرقة أو انتحال هوية.

انتحال الهوية Identity Theft

محاولة سرقة واستخدام المعلومات الشخصية للمستخدم الذي تحدد هويته، وبياناته، ومكان وجوده، للإضرار به، أو الاحتيال بواسطتها على الآخرين.

القرصنة الإلكترونية Electronic Piracy

عملية دخول غير مصرح به إلى جهاز الحاسوب أو شبكة الإنترنت باستغلال نقاط الضعف في الأنظمة المشغلة لها.

البرامج الضارة Malware

مجموعة من البرمجيات التي صممت لغرض إلحاق الضرر بأجهزة الحاسوب والمستخدمين كالفايروسات، والديدان، وأحصنة طروادة، والتجسس.

الابتزاز الإلكتروني Online Blackmail

عملية تهديد وتخويف المستخدم بنشر صور له أو أفلام أو تسريب معلومات سرية مقابل دفع المال أو استغلاله للقيام بأعمال غير قانونية لصالح المبتزين.

التصيد الاحتيالي Phishing Scams

عملية خداع المستخدمين بإرسال رسائل بريد إلكتروني أو تصميم مواقع مزورة لسرقة كلمات المرور، وأرقام الحسابات المصرفية، أو تنزيل البرامج الضارة على الحاسوب.

انتزاع الفدية Ransomware

نوع من البرامج الضارة يعمل على قفل الملفات أو تشفيرها في جهاز المستخدم بحيث لا يمكنه استخدامها إلا بعد دفع مبلغ الفدية، ويكون الدفع عادة في شكل عملة مشفرة.

شكل (6-3): أنواع التهديدات الرقمية الشائعة عبر شبكة الإنترنت

اختبر معلوماتك عن أنواع التهديدات الرقمية الشائعة عبر شبكة الإنترنت، واكتب كل مفهوم في التصنيف المناسب له:

البرامج الضارة	الهندسة الاجتماعية	الابتزاز الإلكتروني	انتزاع الفدية
القرصنة الإلكترونية	انتحال الهوية	التصيد الاحتيالي	

م	الممارسة الرقمية السلبية	تصنيفها
1	توجيه الاتهام إلى شخص بإحدى وسائل التواصل الاجتماعي بفعل لم يقم به وذلك لأهداف شخصية.	
2	الدخول عنوة إلى جهاز شخص آخر عبر شبكة الإنترنت للحصول على معلوماته.	
3	إرسال برنامج ضار إلى جهاز شخص آخر لإغلاقه، والمطالبة بمبلغ مالي مقابل فتح الجهاز.	
4	ملاحقة شخص عبر شبكة الإنترنت للمطالبة بمبلغ مالي مقابل عدم نشر معلوماته.	
5	الاتصال على موظف الدعم الفني، وإقناعه بأنك جديد في الشركة، وأنت لا تملك معلومات الدخول على النظام.	
6	الحصول على معلومات شخص بطريقة غير قانونية، واستخدامها في طرائق غير شرعية كالاختيال والسرقة.	
7	استلام رسالة بالبريد الإلكتروني تحتوي على عرض رحلات مجانية لحضور إحدى مباريات كرة القدم.	
8	إرسال فايروس مرفق بأحد البرامج لإصابة أحد أجهزة الحاسب لمؤسسة تجارية.	
9	التواصل الشخصي مع أحد المشهورين عبر منصة تويتر لمحاولة الحصول على معلومات قد تفيد بالدخول على حساباته.	
10	شراء منتج من متجر عبر شبكة الإنترنت، وعدم استلامه بعد انتهاء فترة الشحن.	
11	الاتصال بك من قبل شخص يخبرك بأنه موظف البنك ويريد منك تحديث كلمة المرور لحسابك البنكي.	



تشمل البرامج الضارة كل من الفيروسات (Virus)، والديدان (Worms)، وأحصنة طروادة (Trojan Horses)، وبرامج التجسس (Spywares) فالفايروس هو برنامج يصيب برامجك وملفات نظام التشغيل لجهازك، والدودة تكرر نفسها في الجهاز حتى تجعله بطيئاً، وتنتشر بين الشبكات، وأما حصان الطروادة فيختفي في الحاسوب لسرقة معلوماتك المهمة، بينما برنامج التجسس يعمل على جمع المعلومات عن نشاطاتك الكاملة في جهازك ويرسلها للمتتبع؛ للتحكم والاستفادة منها.



|| نموذج الحماية من التهديدات الرقمية

ينبغي على المواطن الرقمي لحماية نفسه أن يكون واعياً فطناً، ومتعلماً مستمراً أثناء استخدامه تقنيات شبكة الإنترنت، وتحقق الحماية بتطبيق نموذج الحماية المتكاملة والمكون من نوعين كما يشير إليها شكل (7-3).



شكل (7-3): نموذج الحماية الرقمية المتكاملة



أولاً: تنمية الوعي بالحماية الذاتية من التهديدات الرقمية

تدريب



قيّم ممارساتك الرقمية في مجال الحماية، واجمع نقاطك التي حصلت عليها لتعرف مستوى حمايتك وفق التقييم الآتي: (15 فأعلى = حماية عالية، 9 إلى 14 = حماية متوسطة، أقل من 9 = تحتاج إلى مراجعة ممارساتك في الحماية)

م	الممارسة الرقمية	النقاط نعم = 1 لا = صفر
1	عندما افتح رسالة بريد إلكتروني وأجد إعلاناً عن عرض مغري لمنتج، فإنني أزور موقع الشركة للتأكد من العرض، ولا أضغط على الإعلان مباشرة.	
2	عندما تصلني رسالة نصية بها رابط لتحديث بياناتي البنكية، فإنني لا أضغط مباشرة على الرابط الموجود في الرسالة إلا بعد التحقق منه.	
3	أتحقق من المعلومات والروابط المرسلة في تطبيق الواتساب من مرسلها قبل فتحها.	
4	إذا أردت زيارة موقع ما، فإنني أبحث عن اسم الموقع متبوعاً باللاحقة مباشرة مثل (Google.com).	
5	لا أحفظ كلمة المرور في جهاز حاسوب عام أثناء تسجيل الدخول لأحد حساباتي.	
6	لا أقوم بتنزيل مرفقات البريد الإلكتروني عندما يتم إرسالها لي من شخص مجهول.	
7	أتجنب الروابط التي تطلب مني تسجيل الدخول أو إعادة تعيين كلمة المرور في بريدي الإلكتروني عندما تطلب من غير الجهة الخاصة بها.	
8	لا أتفاعل مع إعلانات النوافذ المنبثقة (pop-ups) التي تظهر على المتصفح.	
9	لا أشارك كلمات المرور الخاصة بي مع أقرب الناس حولي.	
10	أحدث أنظمة التشغيل مباشرة عندما يصلني تحذير بوجود ثغرات في النظام.	
11	أفحص عنوان البريد الإلكتروني المرسل لي عندما ينتابني الشك في وضع الرسالة البريدية.	
12	إذا أعجبني منتج ما، فإنني أبحث عن اسم الشركة، ومقرها المكاني، وتقييمها من قبل العملاء السابقين.	
13	لا أكتب كلمات مرور سهلة أو مكررة لحساباتي الشخصية لتجنب اختراقها.	
14	لا أقوم بتحميل البرمجيات ومقاطع الفيديو والصور من مواقع مجهولة المصدر.	
15	أضع كلمة مرور لشبكة الواي فاي (Wi-Fi) في منزلي.	



م	الممارسة الرقمية	النقاط نعم = 1 لا = صفر
16	لا أفتح المواقع المحجوبة لاكتشاف ما بها.	
17	لا ألتجوب مع طلبات الأشخاص الغرباء في الألعاب الإلكترونية عبر الإنترنت.	
18	لا أضغط على أي رابط فيه اسم الموقع غير واضح ومباشر.	
19	لا أضغط على رابط لاسم موقع غير متبوع باللاحقة مباشرة مثل: .com, net, gov.	
20	لا اتصل بشبكة واي فاي (Wi-Fi) مفتوحة عندما تكون متاحة لدي.	
مجموع النقاط		
النتيجة		



لزيادة وعيك بالحماية من التهديدات الرقمية، شاهد المقطع المرئي بمسح رمز الاستجابة السريع

كن ذكياً وواعياً لنقراتك (Clicks) أثناء استخدامك لخدمات شبكة الإنترنت بكافة أنواعها، فهي من أهم خطوات حمايتك.



إضاءة

تعاملك الاحترافي مع التقنية الرقمية لا يعد كافياً مقابل مدى وعيك تجاه الأمان والمسؤولية لممارساتك في شبكة الإنترنت.



إضاءة



وزارة التعليم

Ministry of Education

2023 - 1445

نصائح لتعزيز الحماية الذاتية الرقمية



شكل (8-3): نصائح لتعزيز الحماية الذاتية الرقمية

ثانياً: وسائل تطبيق الحماية من التهديدات الرقمية باستخدام البرمجيات والتطبيقات

توجد عدة وسائل لحماية كل من أجهزة الحاسوب المتعددة، وأنظمة التشغيل، والبرمجيات، والتطبيقات والمعلومات، يمكن عرضها فيما يأتي:



- **إنشاء كلمات مرور آمنة:** يجب أن تكون معقدة وطويلة، ومكونة من أحرف اللغة الإنجليزية الكبيرة والصغيرة، والأرقام، والرموز، بحيث يصعب كشفها من قبل برامج التخمين التي يستخدمها المخترقون (سيتم التوسع بها في الدرس اللاحق).

- **إجراء النسخ الاحتياطي (Backup):** ويكون للمعلومات الرقمية المحفوظة على الجهاز مثل: الصور، المستندات، المقاطع المرئية، بيانات التطبيقات، ويتم حفظها في وسائط تخزين داخل الجهاز، أو عبر وسائط تخزين خارجية، أو عبر التخزين السحابي. يمكن استعادة النسخ الاحتياطية في حالة تعرض الجهاز إلى السرقة أو التلف أو تعطل في نظام التشغيل الخاص به.



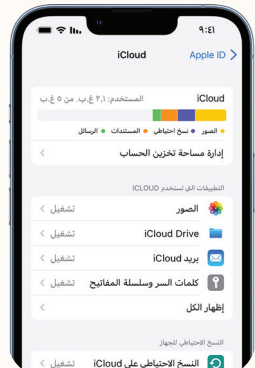
خطوات إجراء النسخ الاحتياطي



نظام التشغيل ويندوز (Windows):

1. انقر على قائمة (ابدأ).
2. اختر (إعدادات Setting).
3. اختر (النسخ الاحتياطي Backup).

شكل (9-3): نافذة إجراء النسخ الاحتياطي لنظام التشغيل ويندوز (Windows)



نظام تشغيل الهاتف الذكي (Apple IOS):

1. انقر على (الإعدادات).
2. سجل دخولك في حساب (Apple ID).
3. اختر (iCloud).
4. حدد المحتويات التي تريد حفظ نسخة احتياطية منها.

شكل (10-3): نافذة النسخ الاحتياطي لنظام تشغيل الآي أو أس



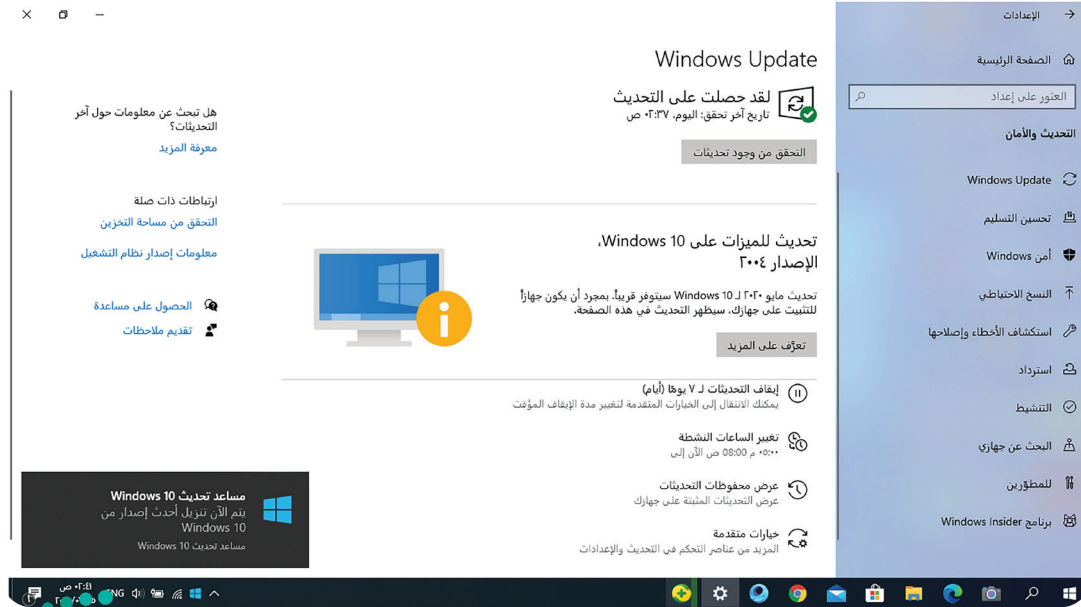
نظام تشغيل الهاتف الذكي (Android):

1. اضغط على (الإعدادات).
2. اختر (النسخ الاحتياطي Backup) من القائمة.
3. حدد المحتويات التي تريد حفظ نسخة احتياطية عنها.

شكل (11-3): نافذة النسخ الاحتياطي لنظام الأندرويد

1. طبق خطوات النسخ الاحتياطي لجهازك الحاسوب أو لهاتفك الذكي حسب الخطوات المذكورة أعلاه.
2. دوّن ملاحظاتك فيما يلي:
 - المدة المستغرقة في عملية النسخ الاحتياطي:
 - نوع الملفات التي تم الاحتفاظ بها في عملية النسخ الاحتياطي:
 - مكان الاحتفاظ بالنسخة الاحتياطية:
3. شارك بياناتك مع زملائك في مدونة المجموعة.

■ **تحديث أنظمة التشغيل:** يقوم مجرمو الإنترنت باختراق الأجهزة عبر الثغرات في الأنظمة والتطبيقات التي تظهر مع مرور الوقت، وتحتوي التحديثات على ترفيقات أمنية لإغلاق الثغرات، فتحديث أنظمة التشغيل من أهم خطوات الحماية، وتشمل عملية تحديث أنظمة التشغيل لكل الأجهزة، والبرمجيات، والتطبيقات، ويُنصح بأن تكون التحديثات تلقائية بدون تدخل المستخدم.



شكل (3-12): نافذة إجراء التحديث لنظام التشغيل ويندوز (Windows)

- نظام التشغيل (Windows): من قائمة (ابدأ) اكتب في محرك البحث (Windows Update)، واختر البرنامج من ضمن قائمة نتائج البحث انظر شكل (3-12)، واكتب رقم نسخة نظام تشغيل الويندوز قبل التحديث وبعده، شارك المعلومة مع معلمك.
- نظام التشغيل (Apple IOS): افتح (الإعدادات) اختر (عام) ثم اختر (تحديث البرامج).
- نظام التشغيل (Android): افتح (الإعدادات) اختر (الأمان) ثم اختر (تحديث الأمان).

شكل (3-13): طريقة فحص الأقراص لاكتشاف الفيروسات في نظام ويندوز (Windows)

بالرجوع إلى شبكة الإنترنت، قارن بين أفضل خمسة برمجيات لمكافحة الفيروسات الحاسوبية من شبكة الإنترنت، وشارك نتيجة بحثك مع زملائك في مدونة المادة.

1.
2.
3.
4.
5.

بعد تثبيت برنامج مكافحة الفيروسات لأول مرة على أحد أجهزتك، قم بإجراء «فحص كامل» للنظام للتأكد من خلوه من الفيروسات، ثم قم بعمليات فحص منتظمة مع مرور الوقت. يفضل ضبط إعدادات البرنامج على (التحديث التلقائي) للبحث بشكل تلقائي عن التحديثات من موقع الشركة.



إضاءة

■ تنشيط المصادقة متعددة العوامل (Multi-factor)

(Authentication): تتضمن الطرق الحديثة أثناء

إنشاء الحسابات في مواقع شبكة الإنترنت بتفعيل المصادقة متعددة العوامل (المصادقة الثنائية الأكثر شهرة)، حيث يصعب وصول المخترقون إلى الحسابات الشخصية، كالبريد الإلكتروني، والحسابات المصرفية، وحسابات شبكات التواصل الاجتماعي، والدخول لأنظمة التشغيل الذكية.



يتم طلب المصادقة متعددة العوامل أثناء تسجيل الدخول لأي خدمة رقمية، وتتنوع المصادقة متعددة العوامل لأنواع عدة: كالرسالة النصية، رسالة البريد الإلكتروني، رقم التعريف الشخصي، البطاقة الذكية، بصمة الوجه، أو تطبيق

لمصادقة التحقق يتم تثبيته سابقاً من قبل المستخدم، ومن أمثلتها التطبيقات: (Microsoft Authenticator, Google)

(Authenticator).

ماذا تفعل أثناء إصابة جهازك بالبرامج الضارة؟

- 1 غير كلمات المرور لحساباتك في أقرب وقت.
- 2 إذا كان برنامج فدية لا تستجيب له.
- 3 تأكد من عدم تضرر النسخة الاحتياطية.
- 4 افحص جهازك.
- 5 فكر كيف تمت إصابتك!
- 6 انشر توعية عن تجربتك.

شكل (3-14): الخطوات المتبعة أثناء الإصابة بالبرامج الضارة

بطاقة المواطن الرقمي للحماية من التهديدات الرقمية

بعد الانتهاء من تعلّم خطوات الحماية في العالم الرقمي، وتحت إشراف معلمك، أكمل الجدول (2-3) الآتي:

جدول (2-3): بطاقة المواطن الرقمي للحماية من التهديدات الرقمية

م	الخطوة	هل تم تنفيذ الخطوة		نوع الأجهزة/ الأنظمة التي تمت حمايتها	تاريخ التنفيذ
		نعم	لا		
1	استخدم كلمة مرور آمنة لحمايتي.				
2	أجري نسخاً احتياطياً لبياناتي في أجهزتي المختلفة.				
3	أجري تحديثاً لنظام التشغيل في جهازي.				
4	أجري تحديثاً للبرامج والتطبيقات عندما تطلب الشركات ذلك.				
5	أفعل التحديث التلقائي لأجهزتي.				
6	أنشأت برامج مكافحة الفيروسات في أجهزتي.				
7	أنشأت المصادقة الثنائية لحساباتي في شبكات التواصل الاجتماعي.				



- أيهما تختار (البرمجيات غير المدفوعة) أم (البرمجيات المدفوعة)، إذا علمت بأن البرمجيات المدفوعة تعطي درجات حماية أعلى بكثير من البرمجيات غير المدفوعة.
- تأمل، هل تكفي الحماية بالمصادقة الثنائية في الوقت الحاضر بعد تطور وسائل الاختراق؟
- فكّر دائماً وتأمل! ... هل الحماية بالبرمجيات والتطبيقات تكفي عن الحماية الذاتية، أم يجب تكامل الاثنين مع بعضهما البعض.

- قد تختلف إصدارات أنظمة التشغيل في الأجهزة الحاسوبية والأجهزة الذكية عن بعض ما تم شرحه في الكتاب، تستطيع البحث عن آليات الفحص والنسخ الاحتياطي عبر شبكة الإنترنت.
- من الأهمية استشارة ذوي الخبرة من الزملاء، الأقرباء، المعلمين، المختصين في مجال التقنية بمجرد الشك بالتعرض لمواقف خطرة أثناء استخدام شبكة الإنترنت.
- قد تختلف طرائق الحماية من نظام لآخر، ومن جهاز لجهاز آخر، دورك في أن تكون سباقاً بأخذ الاحتياطات اللازمة لحماية نفسك وبشكل مستمر، فالعلم يتطور بشكل دائم.



مشروع الدرس



بعد دراستك لوسائل الحماية باستخدام البرمجيات والتطبيقات، وعملاً بحديث الرسول ﷺ: **(أحبُّ الناسِ إلى الله أنْفَعُهُمْ لِلنَّاسِ)**. [أخرجه الطبراني: 6026]، قدّم عملاً كمواطن رقمي تفيد مجتمعك به. نسّق مع معلّمك، ونفّذ إحدى المهمات الآتية:

المهمة الأولى:

- **الموضوع:** اشرح خطوات تحديث أنظمة التشغيل للهواتف الذكية.
- **الهدف:** توعية مجتمعية.
- **طريقة التنفيذ:** اختيار نظامين لتشغيل الهواتف الذكية على الأقل، صمم رسم معلوماتي (Infographic)، باستخدام الصور والمعلومات النصية، والرسومات الجمالية.
- **طريقة التقديم:** مدونة المادة - إحدى وسائل التواصل الاجتماعي.

المهمة الثانية:

- **الموضوع:** إنتاج مقطع فيديو قصير لشرح طريقة تثبيت برنامج مكافحة الفيروسات في جهاز الحاسوب.
- **الهدف:** توعية مجتمعية.
- **طريقة التنفيذ:** باستخدام أحد أدوات مونتاج المقاطع المرئية سواء (برمجيات، موقع إنترنت)، المدة المقترحة لا تقل عن دقيقتين.
- **طريقة التقديم:** الرفع على قناة يوتيوب أو إحدى وسائل التواصل الاجتماعي، نشر المقطع المرئي، إرسال الرابط لحسابك على المعلم.

المهمة الثالثة:

- **الموضوع:** آلية تنشيط المصادقة الثنائية لبعض حسابات وسائل التواصل الاجتماعي.
- **الهدف:** توعية مجتمعية.
- **طريقة التنفيذ:** اختيار ما لا يقل عن (3) حسابات وسائل تواصل اجتماعي، تدريب مجموعة من الطلاب في معمل الحاسوب المدرسي.
- **طريقة التقديم:** جهاز حاسوب - جهاز العرض المرئي (Data Show)، توثيق العمل (صور، مقطع مرئي) وتسليمه للمعلم.



الخصوصية وحماية البيانات

الدرس الثالث

مخرجات التعلم:



- أفرق بين معلوماتي الشخصية ومعلوماتي الخاصة أثناء استخدام شبكة الإنترنت.
- أتعرف على المفاهيم المتعلقة بالخصوصية.
- أبين أهمية حماية خصوصيتي كمواطن رقمي.
- أكتشف أساليب طعم النقرات في إعلانات شبكة الإنترنت.
- أطبق وسائل حماية خصوصيتي أثناء استخدام مواقع الإنترنت وتطبيقاته.
- أنشئ كلمات المرور قوية لحماية خصوصيتي في شبكة الإنترنت.
- أتعرف على تقنيات تشفير البيانات.
- انشر الوعي عن الخصوصية وحماية البيانات في العالم الرقمي.

مصطلحات الدرس:

- المعلومات الشخصية (Personal Information).
- المعلومات الخاصة (Private Information).
- التعقب عبر الإنترنت (Online Tracking).
- الخصوصية (Privacy).
- الإعلان الموجه (Targeted Advertising).
- ملفات الارتباط (Cookies).
- فجوة الفضول (Curiosity Gap).
- سياسة الخصوصية (Privacy policy).
- حماية البيانات (Data Protection).
- شروط الخدمة (Terms of Service).
- تشفير البيانات (Data Encryption).
- طعم النقرات (Clickbait).

التهيئة

شاهد خالد أثناء زيارته مع زملاء مدرسته في الرحلة الصباحية للمؤتمر التقني العالمي ليب (LEAP) المقام في مدينة الرياض نوعاً معروضاً من النظارات التقنية الحديثة، فأعجب بها، وعندما عاد خالد إلى المنزل بدأ بالبحث عبر شبكة الإنترنت عن هذه النظارة لمعرفة كل من: رقم الإصدار، مكان الصناعة، السعر، وبعد الانتهاء من عملية البحث رفع على حسابه عبر منصة تويتر (Twitter)، ومنصة انستجرام (Instagram) عدة صور للنظارة ليستفسر من متابعيه عنها، تفاجأ في اليوم التالي عند دخوله شبكة الإنترنت ظهور إعلانات لهذه النظارة في كل وسيلة من وسائل التواصل الاجتماعي، ومواقع الإنترنت، ومحركات البحث، ورسائل تصله على بريده الإلكتروني، وأخذ في التساؤل عن هذا الوضع، هل هي مصادفة أم لا!!

بعد قراءتك للنص السابق، فكّر في الأسئلة الآتية:

- كيف استطاعت شركات الإعلانات معرفة اهتمام خالد في النظارة؟
- كيف ظهرت كل هذه الإعلانات في فترة واحدة ووقت واحد؟
- كيف يتصرف خالد لو أراد ألا يتعرض لمثل هذا الموقف مرة أخرى؟
- هل تتوقع أن خالد تعرض لانتهاك خصوصيته؟
- هل تؤيد أن تجمع المواقع معلومات عنك وتشاركها مع الآخرين؟ ولماذا هي مهمة بالنسبة لهم؟ ولماذا نستخدم هذه المواقع معلوماتك التي جمعناها منك؟

المعلومات الشخصية (Personal Information) والمعلومات الخاصة (Private Information)

نشاط فردي



16-3

هل تتذكر معلومات خاصة بك سبق أن نشرتها، وشاركتها مع الآخرين عبر شبكة الإنترنت، اذكرها وبين سبب/أسباب

مشاركتها؟

نوع المعلومات:

أسباب المشاركة:

يواجه كثير من مستخدمي شبكة الإنترنت عددًا كبيرًا من المواقع والتطبيقات التي تطلب عملية التسجيل لتمكين خدماتها، ويقف المستخدم حائرًا بين المعلومات التي يطلبها مقدمي الخدمات منهم، ونوع المعلومات التي يجب الإفصاح عنها، إلا أن المواطن الرقمي يجب أن يكون واعيًا للمعلومات التي يفصح عنها، وأن يميّز المواقع والتطبيقات التي يجب عليه إعطاء معلوماته لها أو منعهم منها، ولهذا يجب أن يفرّق بين نوعين من المعلومات: المعلومات الشخصية (Personal Information) وهي معلومات الفرد التي لا تدل على هويته بشكل مباشر، وقد تنطبق على أشخاص آخرين، وتعد معلومات عامة كالهوايات، الأكل المفضل، نوع السيارة، مدينة السكن، نوع جهاز الهاتف الذكي وغيرها، بينما المعلومات الخاصة (Private Information) تدل على هوية الشخص بشكل مخصوص كونها فريدة له كالاسم الكامل، وعنوان المنزل، ورقم البطاقة المدنية، وأرقام الهواتف وغيرها من المعلومات التي ينفرد بها صاحبها دون غيره.

نشاط



بعد معرفتك الفرق بين المعلومات الشخصية والمعلومات الخاصة، حلل إجابتك في نشاط (3-16) بتصنيف نوع المعلومات التي ذكرتها إلى معلومات (شخصية أو خاصة)، وتأمل هل ستعود إلى نشرها مرة أخرى.

المعلومات الشخصية	المعلومات الخاصة
رأيك في العودة لنشرها مرة أخرى	

نشاط



افتراض أنك تريد التسجيل في موقع إنترنت مختص بتصميم بطاقات المعايدة، وتمّ طلب معلومات كاملة عنك، صنّف نوع المعلومات المطلوبة كما في الجدول أدناه إلى معلومات (شخصية أو خاصة)، وبيّن إمكانية مشاركتها عبر هذا الموقع من عدمها.

البيانات	نوع المعلومات (شخصية / خاصة)	إمكانية المشاركة (يمكن / لا يمكن)
اسمك الكامل (Full Name)		
لقبك في الإنترنت (Nickname)		
تاريخ ميلادك (Date of Birth)		
بريدك الإلكتروني (E-mail)		
اسم مدرستك (School Name)		
عنوان منزلك (Home Address)		
هواياتك (Hobbies)		
صورتك الشخصية (Personal Picture)		
طعامك المفضل (Favorite Food)		
نوع الجهاز المستخدم (Device type)		



تقليل الإفصاح عن معلوماتك في مواقع وخدمات شبكة الإنترنت قدر المستطاع؛ يزيد من مستوى حمايتك

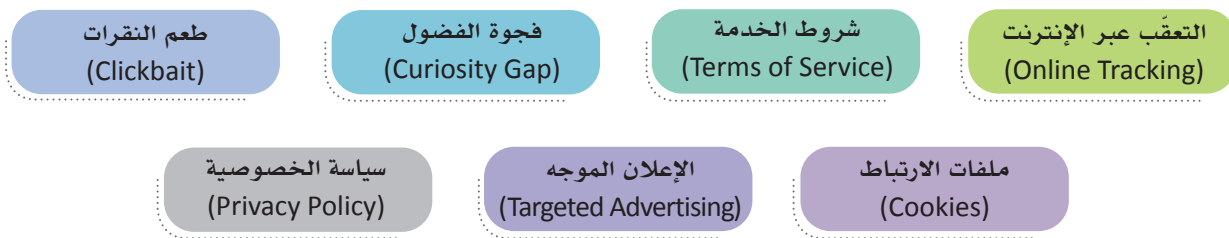
إضاءة

التعامل مع الخصوصية أثناء استخدام شبكة الإنترنت

احترام الخصوصية واجب ديني وأخلاقي، وهو من المبادئ التي حثنا عليها الدين الإسلامي، قال تعالى: ﴿وَلَا يَجَسَّسُوا﴾ [الحجرات: 16]. تعد الخصوصية حق من حقوق الإنسان بموجب كثير من المعاهدات الدولية، وتتنوع الخصوصية كالحق في عدم المراقبة، والقدرة على الحفاظ على سرية الأفكار، والمعتقدات، والهوية، والسلوك، والحق في الاختيار والتحكم في متى وماذا ولماذا وأين وكيف وللمن يتم الكشف عن المعلومات الشخصية، وإلى أي مدى يتم ذلك.

اتجهت الدراسات والأبحاث المالية لتتبع سلوك المستخدم الرقمي لجمع المعلومات عنه لتساعد في تطوير خدمات شركات التقنية لزيادة طرائق الربح، وزيادة العوائد المالية من هذه الخدمات، ولما للتقنيات الرقمية من ضرورة في حياة الفرد اليومية؛ أصبحت حماية الخصوصية للمستخدمين ضرورة ملحة للحد من تعدي الجهات التجارية، فالخصوصية (Privacy) في العالم الرقمي هي حق المستخدم في حماية معلوماته ونشاطاته وتحركاته في شبكة الإنترنت، والتحكم في نشر معلوماته أو منعها. على المواطن الرقمي معرفة كيفية حماية خصوصيته، والاستفادة الكاملة من الخدمات التقنية بدون التعرض لأي ممارسات قد ينتج منها ضرر على نفسه، أو معلوماته، أو أمواله.

المفاهيم المتعلقة بالخصوصية عبر شبكة الإنترنت



شكل (3-15): المفاهيم المتعلقة بالخصوصية عبر شبكة الإنترنت

للتعرف أكثر على معاني المفاهيم السابقة، والتي تسهم في تعزيز حماية الخصوصية أثناء استخدام شبكة الإنترنت،

اقرأ النص الآتي:



تصفح عبد الله ذو الثمانية عشرة عاماً إحدى مواقع شبكة الإنترنت، فوجد إعلاناً على جانب الصفحة كما يظهر في شكل (3-16)، وحينما أثاره الفضول نقر على الإعلان لاكتشاف محتواه، فنقله إلى صفحة موقع يظهر بها محتوى لإحدى تطبيقات التواصل المرئي المباشر غير المشهورة، ثم ظهرت له (نافذة منبثقة) على الصفحة تطلب من عبدالله الموافقة على استخدام ملفات الارتباط التي تخزن في المتصفح، وبعد الموافقة ظهرت نافذة أخرى تطلب منه النقر لتثبيت التطبيق على جهازه، وبعد التثبيت، ظهرت شروط استخدام التطبيق التي تجاوزها عبدالله ولم يقرأها، ثم ظهرت له نافذة أفصحت الشركة عن سياستها في التعامل مع بيانات المستخدمين، فوافق عليها كذلك بدون قراءتها، وبعد تسجيل بياناته وفتح التطبيق تفاجأ عبدالله بأن نوع التواصل خادش للحياة، ومنافياً لقيم الدين الإسلامي، وبشكل دوري أصبح يستقبل عبدالله على رقمه رسائل نصية من أرقام خارجية تحمل روابط مختصرة مثيرة للشك، وظهور إعلانات للتواصل في حساباته على وسائل التواصل الاجتماعي، ويستقبل على بريده الإلكتروني إعلانات عن محتويات باللغة الإنجليزية غير مفهومة بالنسبة له، بالإضافة لظهور محتويات غير أخلاقية متضمنة بهذه الرسائل، وانزعج عبدالله من هذه الخدمة وقرر حذف التطبيق بشكل نهائي.

شكل (3-16)



اضغط وانطلق - حلق عبر العالم الكوني الكبير
ينتظرونك هناك - ماذا تنتظرون!

1. تمعن في النص أعلاه، وحاول أن تربط المواقع والأحداث المذكورة وتوصيلها بالمفاهيم وتعريفاتها.

(ج) تعريف المفهوم	(ب) المفهوم	(أ) المواقف والأحداث في القصة
توجيه الإعلانات للمستخدم بناءً على المعلومات التي جُمعت منه.	سياسة الخصوصية	الإعلان الجذاب على جانب الصفحة
التعرف على نشاطات المستخدم كالمواقع التي زارها، والروابط التي نُقرت، ومدة استخدام المواقع والتطبيقات والتي تجمع من قبل أصحاب المواقع والتطبيقات وجهات الطرف الثالث (Third-Parties).	ملفات الارتباط	إثارة فضول عبدالله بالتعرف على محتوى الإعلان
رغبة كل شخص في اكتشاف المعلومات المفقودة.	شروط الخدمة	الموافقة على تحميل ملفات الارتباط في المتصفح
مستند قانوني يجب أن يوفره مالك التطبيق أو موقع الإنترنت، يصف القواعد التي يجب على الشركة والمستخدمين الالتزام بها أثناء الاستخدام.	الإعلان الموجه	ظهور شروط استخدام التطبيق
ملفات نصية صغيرة مخزنة على جهاز كمبيوتر تتعقب ما يفعله الشخص على موقع ويب في شبكة الإنترنت.	طعم النقرات	نافذة إفصاح الشركة عن سياستها في التعامل مع بيانات المستخدمين
صورة أو عنوان رئيس يحاول حثك على النقر عليه، عادةً لأغراض الدعاية.	التعقب عبر الإنترنت	ظهور الإعلانات المتكررة في حسابات المستخدم في منصات التواصل الاجتماعي
وثيقة قانونية يجب أن يوفرها التطبيق أو موقع الويب والتي توضح معلومات المستخدم التي يجمعونها وكيف استخدموها.	فجوة الفضول	إرسال الرسائل النصية والبريد الإلكتروني المتعدد المحتويات

2. بناءً على قراءة النص السابق، حلّ وأجب عن الأسئلة الآتية:

أ. ما موقف عبدالله من التطبيق؟، وما الاحتياطات التي كان يجب عليه إجراؤها قبل استخدامه؟

ب. برأيك كيف وصلت شركات الإعلانات إلى حسابات عبدالله المختلفة؟

ج. إذا أراد عبدالله عدم تعقبه مرة أخرى، ما الإجراء الذي سيتخذه في مثل هذه الحالة؟

د. هل تتوقع أن للتطبيق آثارٌ على خصوصية عبدالله بعد حذفه؟ وضح إجابتك مع ربطها بمفهوم البصمة الرقمية كما درست سابقاً.



طعم النقرات (Clickbait)

يستخدم البعض من مالكي المواقع والتطبيقات وشركات الإعلانات مفهوم طعم النقرات (Clickbait) في الإعلانات إثارةً لاهتمام المستخدم بجعله أكثر تشويقاً وفضولاً لاكتشاف ما يوجد خلف الإعلان، ويتم ذلك بالمبالغة في صياغة عنوان الإعلان، وحبك تصميمه ليدفع المستخدم على نقر الإعلان للتوجه إلى الهدف المقصود، ويكمن الجانب الأخطر لهذه الطريقة وجود ممارسات ضارة بربط الإعلان بصفحة تحتوي على ملفات ضارة تصيب جهاز الحاسوب، أو سرقة المعلومات واستغلالها في تنفيذ التصيد الاحتيالي، أو جمع المعلومات لغرض بيعها لطرف ثالث كشركات الإعلانات، بالإضافة إلى الكسب المادي لعدد النقرات التي تصاحب الإعلان. يجب على المواطن الرقمي أن يكون واعياً بعدم الانجراف وراء العناوين المضللة التي تثير الفضول حتى لا يتعرض للخداع، وعدم النقر على كل إعلان لا فائدة منه. لمعرفة ما إذا كان الإعلان طعمًا مضللًا؛ يجب الانتباه إلى كون المعلومة المعروضة واقعية أم من نسج الخيال، وهل تميل إلى الغرابة؟!، وهل يصعب تصديقها في أغلب الأحيان؟!، ويوضح شكل (3-17) بعضًا من الأمثلة على ممارسات طعم النقرات عبر شبكة الإنترنت.

حقق الفوز في هذه اللعبة باستخدام
هذه الحيلة الغريبة.

شاهد اصطدام كوكب القمر بالأرض
قبل 5000 عام.

لن تصدق أبدًا، شاهد كيف تم
اصطياد الحوت بسنارة صيد صغير.

هل تريد أن تكون مليونيرًا في
خمسة أيام. (اضغط هنا)

كثيرًا من الناس لا يعرفون هذا السر
عن المشاهير. تعرف عليه بنفسك.

شكل (3-17): نماذج من إعلانات طعم النقرات



بيّن نوع الإعلانات التي يوجد بها حالة طعم النقرات مع توضيح سبب اختيارك:

التوضيح	وجود حالة طعم النقرات		الإعلان
	لا	نعم	
			 <u>10 أسرار لا تعرفها عن لعبة الجندي المحارب.</u>
			 <u>هل تريد أن تكون من أكثر الناس ثراءً انقر هنا</u>
			 <u>أفضل خمسة أماكن سياحية تستطيع قضاء الوقت بها.</u>
			 <u>هل تريد أن تخفف من وزنك خلال أسبوع اضغط واحصل على البرنامج</u>



|| حماية البيانات (Data Protection)

تعد حماية بيانات الأفراد إحدى أشكال حفظ الخصوصية التي تتعرض للانتهاكات من خدمات شبكة الإنترنت، وتعمل هذه الخدمات على جمع وتخزين وتحليل ومشاركة كميات هائلة من البيانات الشخصية من قرصنة الأشخاص والبرمجيات، والاحتيال لسرقة الهوية والمعلومات الشخصية وحسابات البريد الإلكتروني والصور والفيديو وغيرها. تتم المتاجرة بالبيانات كسلعة أساسية في العصر الحالي بين الشركات، وتعد كذلك هدفًا من أهداف مخترقي شبكة الإنترنت لسهولة الوصول إليها في ظل ضعف حماية الأنظمة، وازدياد عدد الأجهزة المتصلة بالإنترنت، بالإضافة لظهور تقنية إنترنت الأشياء (IoT: Internet Of Things)، وقلة خبرات الأفراد في حماية بياناتهم. يوضح الشكل (18-3) ممارسات الأفراد عبر شبكة الإنترنت التي يتم جمعها وتحليلها من قبل الشركات للكشف عن أنماطهم واتجاهاتهم خاصة فيما يتعلق بالسلوك البشري، والتفاعلات ليتكون لدينا مفهوم البيانات الضخمة (Big Data).

البيانات المحفوظة لممارسات الأفراد في شبكة الإنترنت



شكل (18-3): البيانات المحفوظة لممارسات الأفراد عبر شبكة الإنترنت

تمت أشهر انتهاكات البيانات عبر شبكة الإنترنت باختراق بيانات أكثر من 3 مليارات حساب من مستخدمي موقع Yahoo في العام (2013م)، وتم الوصول إلى بيانات المستخدمين الشخصية، وعناوين البريد الإلكتروني، وكلمات المرور الخاصة بهم (unodc.org).



وسائل تحسين الخصوصية وحماية البيانات أثناء استخدام خدمات شبكة الإنترنت

■ **الوعي:** تتمثل الحماية بوعي الأفراد لممارساتهم أثناء تعاملهم مع مواقع شبكة الإنترنت وتطبيقاتها، لذا فهم مسؤولون بشكل مباشر عن تقليل البيانات التي يوفرونها للآخرين، وإدارة بصمتهم الرقمية بحكمة، وفيما يأتي بعضًا من الوسائل التي تساعد في ذلك:

- اختيار عدم المشاركة في جمع البيانات وتحليلها واستخدامها.
- توفير الحد الأدنى من المعلومات الشخصية المطلوبة لاستخدام وسائل التواصل الاجتماعي.
- قراءة سياسة الخصوصية وشروط الخدمة لكل خدمة يتم التسجيل بها.
- التقليل من المعلومات الشخصية المطلوبة من أجهزة تقنية (إنترنت الأشياء).
- تحديث إعدادات أمان التطبيقات، ومواقع الإنترنت، وغيرها.
- تحديد ما يتم مشاركته من معلومات عند الحاجة الضرورية والمهمة فقط.

■ **ضبط إعدادات الخصوصية في أجهزة الهواتف الذكية:** تتيح إدارة الخصوصية في أنظمة تشغيل الهواتف الذكية إمكانية التحكم في التطبيقات التي يمكنها الوصول إلى المعلومات المحفوظة في جهاز المستخدم كمتبوع المواقع، وجهات الاتصال، والكاميرا، والصور، والمقاطع المرئية وغيرها، وتتم عملية التحكم عبر إعطاء الأذونات للتطبيقات بالسماح لها باستخدام بيانات الجهاز. يبين الشكل (3-19) رسالة طلب الإذن لاستخدام موقع الجهاز على الخريطة المكانية.



شكل (3-19)



■ إزالة ملفات تعريف الارتباط (Cookies)،

وتنظيف الحاسوب من الملفات المؤقتة: يؤدي

تخزين ملفات الارتباط لاستغلال البيانات،

وانتهاك الخصوصية من قبل المخترقين.

يمكن إزالة ملفات ارتباط المواقع من جميع

المتصفحات المشهورة (Microsoft Edge

Google Chrome - Mozilla Firefox) على نظام

التشغيل ويندوز (Windows) بالضغط على (Ctrl

+ Shift + Delete) معاً على لوحة المفاتيح، ويمكن

إكمال خطوات إزالة ملفات التصفح، وملفات



1-حدد الزمن

2-حدد المحذوفات

3-انقر على (مسح الآن)

شكل (20-3): خطوات إزالة ملفات الارتباط للمتصفح

الارتباط، والملفات المؤقتة في متصفح (Microsoft Edge) بالنظر إلى الشكل (20-3).

كما يُظهر الشكل (21-3) طريقة إزالة ملفات الارتباط لمتصفح قوقل كروم (Google Chrome) على نظام تشغيل

الهاتف الذكي بعد الوصول إلى (الإعدادات).



شكل (21-3): إزالة ملفات الارتباط لمتصفح قوقل كروم على الهاتف الذكي.

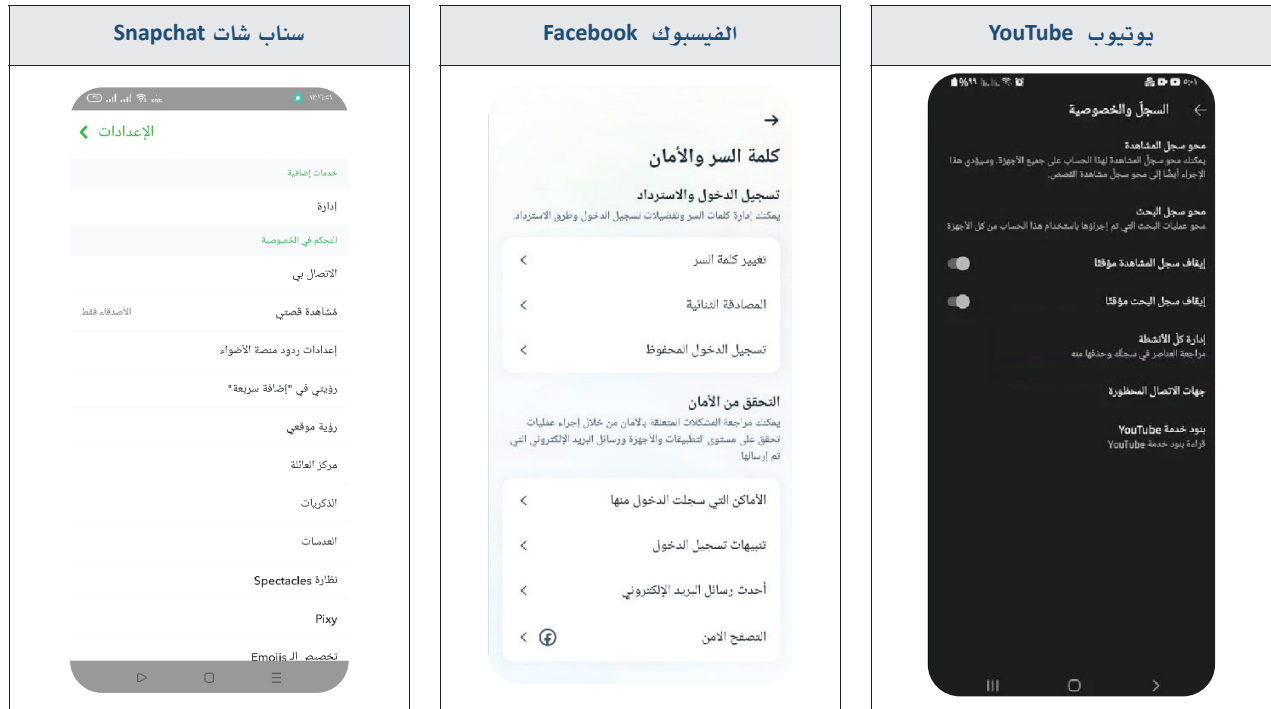
■ **تحسين إعدادات الخصوصية في متصفحات الإنترنت:** يؤدي تحسين إعدادات الخصوصية في المتصفحات إلى التقليل من عمليات التتبع عبر الإنترنت أو حجبها، وكذلك حجب تنزيل ملفات الطرف الثالث على الجهاز، والتحذير من انتهاكات كلمة المرور في حالة اختراقها، والتحكم في عرض النوافذ المنبثقة، وخيارات أخرى. يمكن الوصول لنافذة تحسين إعدادات الخصوصية للمتصفحات عبر اتباع الخطوات في الجدول (3-3).

جدول (3-3): الوصول إلى إعدادات الخصوصية لبعض المتصفحات

المتصفح	الخطوات
	انقر على الثلاث نقاط في أعلى المتصفح ثم اختر (الإعدادات Setting) ثم اختر (الأمان والخصوصية Privacy and Security).
	انقر على الثلاث نقاط في أعلى المتصفح ثم اختر (الإعدادات Setting) ثم اختر (الخصوصية والبحث والخدمات Privacy, search, and services).
	انقر على الثلاثة شرائط في أعلى المتصفح ثم اختر (الإعدادات Setting) ثم اختر (الأمان والخصوصية Privacy and security).
	انقر على (الإعدادات Setting) ثم (الخصوصية Privacy).

■ **ضبط إعدادات الخصوصية في التطبيقات:** تحتوي التطبيقات على إعدادات الخصوصية يمكنك ضبطها للحد من جميع المعلومات، وذلك عبر مراجعة أذونات التطبيقات، فيمكن جعل الحساب خاصاً، وتحديد رفض الوصول إلى معلومات الموقع، وجهات الاتصال، واستعمال الكاميرا، والوسائط المتعددة في الجهاز، كما يمكن التحكم في نوع الإعلانات التي تظهر في التطبيق، وغيرها من الخيارات. على المستخدم قراءة سياسة الخصوصية، وشروط الخدمة التي تتوفر بكل تطبيق لمعرفة ما يتم جمعه من قبل الشركات، وما بصدد المستخدم الموافقة عليه، وتحديد ما يمكن السماح به أو رفضه. يظهر الشكل (3-22) نوافذ إعدادات الخصوصية لبعض تطبيقات وسائل التواصل الاجتماعي.





شكل (22-3): نافذة إعدادات الخصوصية لبعض تطبيقات الهاتف الذكي

تدريب

6-3

طبق وسائل تحسين إعدادات الخصوصية وحماية البيانات على مختلف الأجهزة الرقمية التي تتوفر لديك، وشارك مرئياتك مع زملائك في مدونة المادة.

إرشادات كتابة كلمات المرور الآمنة

ينبغي على المواطن الرقمي أن يتعامل مع كلمات المرور بطريقة واعية، فبعض التطبيقات ومواقع الإنترنت لا تتوفر بها أسلوب المصادقة متعددة العوامل (MFA)، ولهذا فإن اختيار كلمة مرور آمنة هو الخيار الوحيد لحماية المعلومات والحسابات من الاختراق أو الاحتيال أو انتهاك الخصوصية، وكتابة كلمة مرور آمنة بشكل ذاتي من قبل المستخدم أو باستخدام تطبيقات توليد كلمات المرور يجب اتباع الإرشادات الآتية:

- كلما كانت كلمة المرور طويلة كان من الصعب اختراقها (لا تقل عن 10 خانات).
- يفضل استخدام الأحرف الكبيرة والصغيرة والأرقام والرموز مع دمجها بغير ترتيب.



- عند القلق من نسيان كلمة المرور المبعثرة؛ يمكن انشاء كلمات كاملة يمكن تذكرها، على ألا تكون معروفة ومتداولة بين الناس، وفي الوقت نفسه غير مرتبطة بصاحب الحساب كاسمه أو تاريخ ميلاده أو أسماء أحد أفراد أسرته، أو سيارته (لماذا؟).
- تطبيق قاعدة الكلمات المتتالية التي يصعب على الحاسوب تخمينها.
- تجنب استخدام الحروف أو الأرقام المتتالية.

تعمل برامج توليد كلمات المرور على إنشاء كلمات مرور مقترحة بعدة صيغ وباختيارات متعددة، جَرِّب إحداها.



إضاءة

تهدف برامج إدارة كلمات المرور إلى تجميع كل كلمات المرور الخاصة بك في مواقع الإنترنت لديها مع تطبيق تشفير عالي لها، وعند الحاجة لتسجيل الدخول لإحدى المواقع فإنه يدرج اسم المستخدم وكلمة المرور الخاصة به تلقائياً نيابة عنك، علماً بأن برامج إدارة المرور تحتاج إلى كلمة مرور خاصة بها، ويجب كتابتها بعناية متبعاً إرشادات كتابة كلمات المرور في هذا الدرس.



إضاءة

نشاط



21-3

ناقش مع زملائك في الصف، ما المخاطر المترتبة على سرقة كلمات المرور الشخصية منك؟

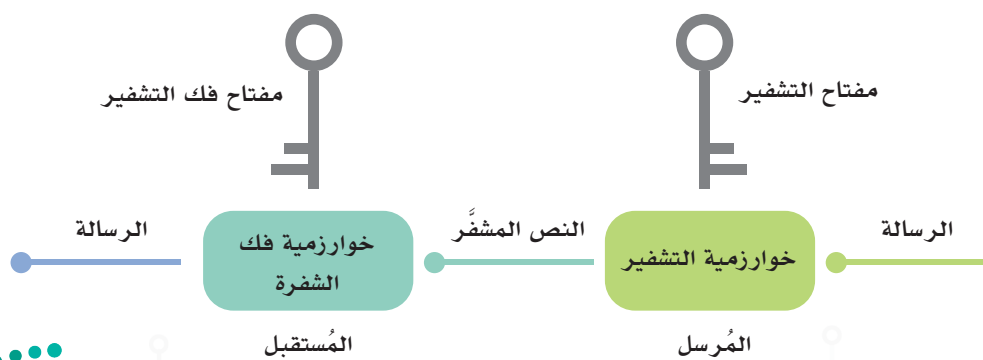


بالعودة لإرشادات كتابة كلمات المرور؛ حدد كلمات المرور الآمنة وغير الآمنة مع ذكر الأسباب.

م	كلمة المرور	آمنة / غير آمنة	السبب/الأسباب
1	abcdefg		
2	Password1		
3	?4ee2#ge?6ng		
4	basketball		
5	84sk37b4LL		
6	12345		

تشفير البيانات (Data Encryption)

يواجه مستخدمو التقنية احتمالية اختراق بياناتهم في شبكة الإنترنت، وعلى المواطن الرقمي محاولة البحث عن التقنيات والآليات التي تساعد في حماية بياناته، ومن أشهر الطرق لمواجهة هذه المشكلة تقنية إخفاء البيانات أو ما تسمى بالتشفير (التعمية)، وتتمثل فكرة التشفير في محاولة إخفاء البيانات المهمة لتظهر بشكل غير مفهوم عند محاولة قراءتها من قبل شخص أو جهة غير مصرّح لهم بالاطلاع عليها وذلك بتغيير شكل الرسالة قبل إرسالها من قبل المرسل، وبعد وصولها إلى المستقبل يتم تحويلها إلى شكلها الأصلي حيث ينفرد بالاطلاع على الرسالة بنصّها الأصلي فقط الطرفين (المرسل، والمستقبل). يشير الشكل (23-3) لمسار نص الرسالة أثناء مراحل التشفير.



شكل (23-3): مسار تشفير الرسالة من المرسل إلى المستقبل

يجري التشفير على البيانات بهيئة نصوص مباشرة أو على هيئة ملفات رقمية (صورة، صوت، فيديو، ملف تنفيذي (exe)، أو على هيئة أرقام ثنائية (الواحد، والصفر)، وعند التشفير يستخدم ما يسمى (بمفتاح التشفير) والذي بدون له تتم عملية تشفير/ فك تشفير البيانات، والمفتاح يكون عادة كلمة المرور مكون من مجموعة من الحروف والأرقام والرموز، ويجب توفره لدى الطرفين (المرسل والمستقبل).

من الضروري حفظ مفتاح التشفير في مكان آمن، بحيث لا يمكن لأحد الوصول إليه، ويجب عدم تخزينه في جهاز الهاتف الخاص بك حتى لا يتم الوصول إليه عند فقدانك للجهاز أو في حالة سرقة منك.



إضاءة

إرشادات تشفير البيانات أثناء استخدام شبكة الإنترنت:

أولاً: التعامل مع المواقع المشفرة على شبكة الإنترنت: تساعد المواقع المشفرة بنقل البيانات وتخزينها بشكل آمن. يتم التحقق من عنوان الموقع (URL) باحتوائه على حرف «s» بعد بروتوكول نقل النص التشعبي (http)، أو بالبحث عن قفل الارتباط الآمن في شريط (URL). تساعد تقنية تشفير الاتصال الآمن في مواقع الإنترنت على عدم قابلية البيانات وجدواها للاستخدام عند تسريبها.

ثانياً: تشفير محركات الأقراص الثابتة، والأقراص القابلة للإزالة: يمكن تشفير القرص الصلب لجهاز الحاسوب بنظام الويندوز لضمان حفظ الملفات عبر برمجية ملحقة لتشفير القرص الصلب تدعى (BitLocker Drive Encryption). وتعمل البرمجية على تشفير القرص، وإغلاقه بكلمة مرور، واسترجاعها في حالة فقدانها.

ثالثاً: تشفير رسائل البريد الإلكتروني: يمكن للمستخدم تشفير رسائله لإخفاء محتوياتها إذا تم اعتراضها من قبل طرف ثالث، وأشهر تقنيات التشفير البريدية المتداولة هي (S/MIME – PGP – TLS)، ويستخدمها أشهر مقدمي خدمة البريد (Outlook, Gmail) وغيرهم، ويشترط مقدمي خدمة البريد الإلكتروني أن تكون تقنية التشفير مفعلة من قبل الطرفين المرسل والمستقبل.



نصائح عامة لتحسين الخصوصية وحماية البيانات أثناء استخدام شبكة الإنترنت

- لا تعيد استخدام نفس كلمة المرور على حسابات متعددة، بل اجعلها فريدة لكل حساباتك (لماذا؟).
- ينبغي عدم حفظ كلمات المرور (ميزة تذكروني) في المواقع والتطبيقات على جهازك أو على جهاز حاسوب عام لهدف الدخول السريع إليها.
- اعمل تسجيل الخروج بعد استخدام حساباتك على أجهزة الحاسوب العامة.
- احذر الاتصال بشبكات الواي فاي (Wi-Fi) العامة فهي غير آمنة على الغالب، وقد تكون وهمية من صنع المخترقين.
- كن حذرًا بشأن المعلومات التي تشاركها في ملفك الشخصي على حساباتك كأسماء الحيوانات الأليفة، والمدارس، وأسماء أفراد الأسرة، فقد تفيد المخترقين في تخمين كلمات المرور الخاصة بك، أو إجابات لأسئلة أمان حساباتك.
- تجنب استخدام محطات الشحن المجانية في المطارات أو الفنادق أو مراكز التسوق -قدر الإمكان-، فهي وسيلة لانتقال البرامج الضارة وملفات التجسس.
- اختر كلمات المرور الخاصة بك بعناية ليصعب على الآخرين تخمينها، واعمل على تحديثها بانتظام.
- لا تسجل بياناتك الشخصية كاملة عندما تُطلب من قبل مواقع وتطبيقات شبكة الإنترنت.
- لا تشارك معلوماتك الشخصية كأرقام الهواتف، وموقع المنزل، وتاريخ الميلاد مع غرباء عبر شبكة الإنترنت، أو مع أشخاص لا يوجد بينك وبينهم معرفة شخصية.
- عطّل ميزة نشر الرسائل على مواقع وسائل التواصل الاجتماعي المتعددة في آن واحد.
- كن واعيًا بآثار الخصوصية للألعاب وتطبيقات الطرف الثالث الأخرى داخل مواقع التواصل الاجتماعي، يمكن لهذه التطبيقات مشاركة المعلومات أو نشرها بشكل افتراضي دون أن يكون المستخدم على علم بها بالضرورة.
- اقفل جهازك الشخصي برمز القفل (PIN) حتى يحمي خصوصيتك من الاطلاع عليها من قبل القرابين منك، أو في حالة فقدته يومًا ما.
- قيّد الوصول إلى تطبيقات جهازك بحيث لا يمكن فتحها إلا من خلالك فقط.
- لا تحدد موقع الجهاز على الخريطة (Map) في نظام التشغيل، وكذلك عند طلبها من قبل تطبيقات الهاتف إلا عند الحاجة.
- استخدم برمجيات حجب الإعلانات (Ad blocking Software) لزيادة حماية الخصوصية لديك.
- لا تثبّت على هاتفك المحمول تطبيقات غير معتمدة أو غير مفحوصة من قبل شركات الهواتف مثل (App Store, Google Play).



- لا تحفظ بيانات دخول الألعاب الإلكترونية وأرقام بطاقات الائتمان داخل التطبيقات الخاصة بها.
- لا تستخدم الاسم الحقيقي ، أو مشاركة مكان الإقامة، أو التواصل مع/أو إضافة الغرباء أثناء اللعب عبر الإنترنت.

بطاقة المواطن الرقمي لتحسين الخصوصية وحماية البيانات في شبكة الانترنت

بعد الانتهاء من تعلّم وسائل تحسين الخصوصية في العالم الرقمي، وبمتابعة من معلّمك في الصف، أكمل

جدول (3-4) الآتي:

جدول (3-4): بطاقة المواطن الرقمي لتحسين الخصوصية وحماية البيانات

م	الخطوة	هل تم تنفيذ الخطوة		ماهي الأجهزة أو الأنظمة التي تمت الحماية بها	تاريخ التنفيذ
		نعم	لا		
1	ضبط إعدادات الخصوصية في أجهزة الهواتف الذكية.				
2	حذف ملفات تعريف الارتباط (Cookies)، وتنظيف الحاسوب من الملفات المؤقتة.				
3	تحسين إعدادات الخصوصية في متصفحات الإنترنت.				
4	ضبط إعدادات الخصوصية في التطبيقات.				
5	إنشاء كلمة مرور قوية.				



- هل هناك تعارض بين تقليل بيانات خصوصيتك عبر شبكة الإنترنت وفي الوقت نفسه زيادة قوة بصمتك الرقمية.
- هل من المفترض أن يكون لديك هويتان رقمية عبر شبكة الإنترنت لحماية خصوصيتك؟
- كيف يمكنك أن تتحقق من بيانات الأشخاص الغرباء عندما يتواصلون معك عبر ألعاب شبكة الإنترنت.

- عند وضع كلمات مرور لحساباتك المختلفة، يجب أن تفرّق بين حساباتك المهمة والأقل أهمية، فكلمات المرور لحساباتك المهمة كالحساب البنكي أو حساب منصة مدرستي أو حساب البريد الإلكتروني الرسمي لديك يجب أن تكون أقوى بكثير من غيرها.
- لا تستخدم عند إنشاء كلمات المرور أية كلمات تدل عليك بشكل مباشر، فهي مطمع من يحاول أن يحتال عليك عبر استخدام مفهوم الهندسة الاجتماعية كما درست سابقاً.
- وعيك كمواطن رقمي السبب الأول لحفاظك على خصوصيتك.
- لا تتردد في قراءة سياسة الخصوصية أو شروط الخدمة لأي من تطبيقات الإنترنت، فهي تعطيك فكرة كاملة عن حقوقك، وكيف يتم استخدام بياناتك.



مشروع الدرس



بالعودة إلى موضوع (نصائح عامة لتحسين الخصوصية وحماية البيانات أثناء استخدام شبكة الإنترنت) نفذ خطوات المشروع الآتية:

- **الموضوع:** تقديم نصائح عن تحسين الخصوصية وحماية البيانات.
- **الهدف:** توعية مجتمعية.
- **طريقة التقديم:**
 - تقديم رسالة نصية بشكل مباشر.
 - تصميم النصائح على هيئة صورة.
 - إنتاج مقطع مرئي قصير.
 - شكل رسومي كخريطة ذهنية.
- **موقع التنفيذ:** استخدام أربعة حسابات للطالب في وسائل التواصل الاجتماعي.
- **خطوات التنفيذ:**
 - اختيار ثمانية نصائح لتقديمها.
 - انشر بشكل يومي.
 - أشر إلى حساب المعلم أثناء عملية النشر.
 - انسخ جزءاً من عملك، وضعه في مدونة المادة / مجموعة المادة.





حماية الملكية الفكرية للمحتوى الرقمي

الدرس الرابع

مخرجات التعلم:

- أتعرف على مفهوم الملكية الفكرية لحفظ حقوق الإبداعية.
- أتعرف على خطوات تسجيل حقوق الملكية الفكرية لبراءات الاختراع محلياً.
- أميز بين أنواع تراخيص المشاع الإبداعي عند رفع أعمال شخصية عبر شبكة الإنترنت.
- أطبق التوثيق الصحيح للمراجع التي أضمنها في أعمالي.
- أفرق بين النزاهة الأكاديمية والانتحال الرقمي للأعمال على شبكة الإنترنت.
- أستشعر التأثير الاقتصادي والاجتماعي السلبي لانتهاك حقوق الملكية الفكرية على الاقتصاد الوطني.
- استنتج الفوائد الإيجابية لحفظ حقوق الملكية الفكرية لتقدم الاقتصاد الوطني.
- أطبق نظام حماية حقوق المؤلف على الممارسات الرقمية للحقوق الفكرية.
- أساهم في نشر التوعية للمجتمع عن أهمية الملكية الفكرية.



مصطلحات الدرس:

- الملكية الفكرية (Intellectual Property).
- الاقتباس (Quoting).
- الانتحال الرقمي (Digital Plagiarism).
- التوثيق (Citation).
- النزاهة الأكاديمية (Academic Integrity).
- براءة الاختراع (Patent).
- ترخيص المشاع الإبداعي (Creative Commons License).

التهيئة

سالم طالب طموح، يهتم دائماً بتطوير نفسه في مجال برمجة تطبيقات الهواتف الذكية، بدأ اهتمامه من خلال دراسته البرمجة في المرحلتين المتوسطة والثانوية، ثم أكملها عبر الالتحاق بالدورات التدريبية عبر شبكة الإنترنت، ويفكر دائماً بإنتاج تطبيقه الشخصي الذي يستثمر فيه خبرته في البرمجة ليواكب شهرة تطبيقات وسائل التواصل الاجتماعي المنتشرة عالمياً، ويدور في ذهنه الأسئلة الآتية:

- هل يحق لي أن أستفيد أفكاراً من التطبيقات المتوفرة لاستخدامها في تطبيقي؟
- كيف أعرف أن استفادتي من أفكار التطبيقات المتوفرة مسموح أم غير مسموح؟
- كيف أحمي نفسي من المساءلة القانونية أثناء الاستفادة من أعمال الآخرين؟
- كيف أستطيع أن أحمي إنتاجي بعد الانتهاء منه؟
- كيف أسجل منتجي النهائي في الجهة الرسمية في الدولة لضمان حمايته؟



الملكية الفكرية والمجالات التابعة لها

يشير مفهوم الملكية الفكرية (Intellectual Property) إلى ما يمتلكه الفرد من إنتاج ابتداءً من الفكرة وما تحمله من ابتكار أو اختراع جديد، ومن ثم الوصول إلى الشكل النهائي لها. يعود هذا الإنتاج لملكية الفرد الخاصة، ولا ينافسه على إنتاجه أي فرد آخر أو جهة، ويكون له الحق في التصرف به، أو التنازل عنه، أو الترخيص للغير بالاستفادة منه أو التطوير عليه. تنهى الشريعة الإسلامية عن التعدي على حقوق الآخرين حماية لإنتاجاتهم كما في قوله -سبحانه وتعالى-:

﴿وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَآ إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ﴾



[البقرة: 188]، ومن هذا المنطلق أولت المملكة العربية السعودية الاهتمام بحماية الملكية الفكرية، وأنشأت الهيئة السعودية للملكية الفكرية (SAIP: The Saudi Authority for Intellectual Property) التي تُشرف على إدارة حماية الملكية الفكرية، ولزيارة موقع الهيئة؛ امسح رمز الاستجابة السريع.

إنراء



تتبع جميع منظمات الحقوق الفكرية للدول الأعضاء في الأمم المتحدة والبالغ عددهم (193) دولة إلى المنظمة العالمية للملكية الفكرية (WIPO)، وتقوم المنظمة بدور ريادي في إرساء نظام دولي متوازن وفعال للملكية الفكرية، يشجع على الابتكار والإبداع والانتفاع من الملكية الفكرية لفائدة الحكومات والشركات والمجتمعات. يمكنك زيارة موقع الإنترنت لمنظمة (WIPO) عبر مسح رمز الاستجابة السريع.

تعرّز حماية الملكية الفكرية حفظ حقوق أصحابها قانونيًا بتأمين العدالة للفرد الذي بذل وقتًا وجهدًا في ابتكار عمل ما بالانتفاع منه ماديًا، وإتاحة المجال للآخرين بالاطلاع عليه، والاستفادة منه مع بقاء اسم المالك ملازمًا للعمل. تغطي حقوق الملكية الفكرية عدة مجالات كما يظهر في الشكل (24-3):

المصنفات الادبية
والعلمية والفنية

براءات الاختراعات

الأداء والبرث الإذاعي
والتلفزيوني

النماذج الصناعية

العلامات التجارية

الاكتشافات العلمية

شكل (24-3): مجالات حقوق الملكية الفكرية



اعتمد صاحب السمو الملكي الأمير محمد بن سلمان آل سعود -ولي العهد حفظه الله- الإستراتيجية الوطنية للملكية الفكرية في عام (2022م)، وتعد الإستراتيجية إحدى ممكنات تحقيق مستهدفات رؤية المملكة 2030، والهادفة إلى بناء منظومة للملكية الفكرية تدعم الاقتصاد القائم على الابتكار، والإبداع، وتحفز التنافسية بينهما، والنمو الاقتصادي. ارتكزت الإستراتيجية على أربع ركائز أساسية هي: توليد الملكية الفكرية، وإدارتها، والاستثمار التجاري لها، وحمايتها. يمكن الاطلاع على الإستراتيجية بمسح رمز الاستجابة السريع.

|| تسجيل حقوق الملكية الفكرية

تهدف عملية حفظ حقوق الملكية لمنتج ما حمايته من التعرض للسرقة الفكرية، وداعمه أثناء التقاضي عند الحاجة لذلك، علمًا بأن القانون يكفل للفرد حماية أعماله مباشرة كحق له، ويعرض الآخرين للمساءلة القانونية عند انتهاك الحقوق. لحفظ الحقوق محليًا يمكن التسجيل إلكترونياً في خدمة (إيداع براءة اختراع) كما في الخطوات الآتية:



1. زيارة صفحة إيداع براءة الاختراع في موقع الهيئة السعودية للملكية الفكرية عبر مسح رمز الاستجابة.
 2. تسجيل الدخول عبر بوابة النفاذ الوطني لحسابات الأفراد، أو إنشاء حساب جديد لدى بوابة الهيئة.
 3. تعبئة البيانات الشخصية لتعريف مقدم الطلب.
 4. تنزيل قوائم الملفات المرفقة بالموقع (الملخص، الوصف الكامل، عناصر الحماية، الرسومات إن وجدت)، وتعبئتها لخدمة (براءات اختراع).
 5. تسجيل بيانات الطلب كاملة، وإعادة إرفاق الملفات المطلوبة سابقًا.
 6. تسديد رسوم الإيداع.
 7. مراجعة الطلب من قبل الهيئة، وإصدار الموافقة عليه.
- كما أشارت المنظمة العالمية للملكية الفكرية (WIPO) إلى بعض الإرشادات لحفظ حقوق العمل الشخصي عند الرفع عبر شبكة الإنترنت، تتمثل الإرشادات كما يوضحها شكل (3-25) الآتي:

3 إدراج قسم في الموقع يحدد فيه طرائق الاستخدام المسموح بها، كالإسماع بالتحميل مع التحذير من البيع، أو التصرف به دون إذن صاحبه.

2 الاحتفاظ بنسخة مطبوعة من العمل الأصلي يظهر به تاريخ نشره لأول مرة.

1 وضع رمز © بجوار اسم صاحب العمل، وسنة إنتاج المصنف، أثناء الرفع للإنترنت.

شكل (3-25): إرشادات (WIPO) لحفظ الأعمال الشخصية أثناء مشاركتها عبر الإنترنت

قد يمنح صاحب العمل إتاحة استخدام أعماله عبر شبكة الإنترنت دون انتهاك للحقوق الفكرية بما يسمى (تراخيص) وذلك لاستفادة الآخرين من هذه الأعمال، أو نقلها، أو التعديل عليها، أو بيعها كذلك، وهنا يتضح الفرق بين العمل المحمي، والعمل المرخص كما سيعرض تفصيليًا في الموضوع اللاحق.

|| تراخيص المشاع الإبداعي (Creative Commons Licenses)

وفرت منظمة المشاع الإبداعي (Creative Commons organization) تراخيص المشاع الإبداعي التي تمنح أذونات حقوق النشر للأعمال الإبداعية من قبل ملاكها بطريقة متعارف عليها بين الجميع، وكما هو معروف فإن أي عمل يكون محمي بحقوق الملكية الفكرية، إلا أن هذه التراخيص تجعل أصحاب الأعمال يوافقون على استخدام أعمالهم ولكن بدرجات متفاوتة في الحقوق، ويجب على من يستفيد من هذه الأعمال أن يحترم هذه الحقوق، ويلتزم بها لئلا يعرض نفسه للعقوبات. توجد ستة أنواع من التراخيص يمكن تضمينها في الأعمال عبر شبكة الإنترنت كما في جدول (3-5).

جدول (3-5): تراخيص المشاع الإبداعي

رمز الترخيص	نوع الترخيص
	للدلالة على نسخ وتوزيع العمل لأي وسط أو شكل مع التعديل والمزج لأي غرض، بما في ذلك بيعه تجارياً.
	للدلالة على نسب العمل لصاحبه الأصلي.
	للدلالة على نسخ المواد وتوزيعها بأي وسيط أو تنسيق في شكل غير مُعدّل (يستخدم العمل كما هو).
	للدلالة على نسخ وتوزيع العمل لأي وسط أو شكل مع التعديل والمزج لأي غرض، ومشاركة التعديلات وفقاً لشروط الترخيص نفسها للعمل الأصلي.
	للدلالة على أن العمل للاستخدام غير التجاري.
	للدلالة على أن العمل لا يخضع لأي شروط وهو متاح في المجال العام.



تدريب



بناءً على أنواع التراخيص في جدول (3-5)، وضح دلالات التراخيص المجمعة فيما يأتي:

رمز الترخيص	نوع الترخيص

نشاط فردي



ابحث عبر شبكة الإنترنت عن ثلاثة أعمال مختلفة (مدونة، صور، تسجيلات صوتية، مقاطع مرئية، مستندات، برمجيات، تطبيقات، غيرها) مرخصة بتراخيص المشاع الإبداعي، واكتب البيانات المطلوبة فيما يأتي:

م	نوع المنتج	مالك العمل	رمز الترخيص
1			
2			
3			

تُلمزمك تطبيقات وسائل التواصل الاجتماعي أثناء التسجيل لديها بالموافقة على الشروط والأحكام الخاصة بالاستخدام، والتي قد تتضمن حصول المنصة منك على ترخيص غير حصري باستخدام منتجاتك التي ألفتها، ونشرتها، أو وضعتها في حسابك بالرغم من احتفاظك بحقوقك الخاصة، ولذلك يجب عليك قراءة الشروط والأحكام لكل البرامج والتطبيقات لمعرفة مضمون الاستخدام لديها.





يوجد تراخيص عدة للبرمجيات الحرة تتبع لمؤسسات غير ربحية، تدعم حرية استخدام برامج الحاسوب والتطوير عليها،

مثل:

(BSD: Berkeley Software Distribution)

(GNU GPL: The GNU General Public License)



النزاهة الأكاديمية مقابل الانتحال الرقمي

اقرأ السيناريو الآتي:

طلب معلّم إحدى المواد الدراسية من طلاب الصف الذي يدرّسه كتابة بحث علمي لإحدى موضوعات المادة، وأشار المعلم لطلابه إلى الالتزام بالقواعد الصحيحة في كتابة هذا البحث وهي كما يلي:

- 1- تحديد موضوع البحث.
- 2- التحلي بالنزاهة الأكاديمية في الكتابة، والبعد عن الانتحال الرقمي.
- 3- البحث في المصادر الموثوقة من الكتب، والمجلات العلمية، ومواقع شبكة الإنترنت المعتمدة.
- 4- كتابة أسماء المراجع التي تمت الاستعانة بها، وتوثيق أسماء الأشخاص الذين تم الاستشهاد بهم.
- 5- تحديد نوع الاقتباس أثناء كتابة التقرير.

كما ورد في السيناريو السابق، ينبغي أثناء القيام بعمل بحث/تقرير علمي من شبكة الإنترنت؛ مراعاة مجموعة من القواعد والضوابط التي تساهم في زيادة إنتاج الأعمال، وتعمل على إرساء مبادئ العدل، والمساواة، وحفظ الحقوق في المجتمعات، ولتحقيق ذلك يجب على الأفراد الالتزام بالنزاهة الأكاديمية (Academic Integrity) التي تعرّف بأنها "الأمانة الفكرية والاستقامة العلمية في استخدام المعلومات ونقلها وتوثيقها ونشرها وإنتاج الأبحاث"، ويقدم المركز الدولي للنزاهة الأكاديمية (ICAI) ستة قيم أخلاقية ينبغي أن يتصف بها المتعلمون في إنتاجاتهم وهي: (الصدق، الشجاعة، الإنصاف، الاحترام، المسؤولية، الشجاعة).

ينافي مفهوم الانتحال الرقمي (Digital Plagiarism) مفهوم النزاهة الأكاديمية، وهو إعادة استخدام فكرة شخص آخر أثناء كتابة عمل ما، ونسبها إلى الشخص المنتحل، ويعد تصرفاً غير مقبول، ويتنافى مع القيم والمبادئ الإسلامية والعلمية، ويعرّض صاحبه إلى انتهاك حقوق الملكية الفكرية، ويقوده إلى المساءلة القانونية، ويظهر شكل (3-26) بعضاً من صور الانتحال.

اقتباس عمل كامل لكاتب ونسبه إلى اسم المنتحل.

تلخيص فكرة لكاتب دون الإشارة لاسمه.

نقل نص معين لكاتب كما هو دون الإشارة لاسمه.

شكل (3-26): بعض صور الانتحال

ولتفادي الوقوع في الانتحال الرقمي أثناء كتابة الأبحاث والتقارير؛ يمكن استخدام الاقتباس (Quoting) الذي يعرف بأنه: اقتباس أفكار كاتب آخر باستخدام الكلمات أو بالأسلوب اللغوي للكاتب، وتوجد ثلاثة آليات للاقتباس يمكن التعامل معها عند الحاجة إلى الاستلهام من أفكار الآخرين وكتاباتهم، مع ضرورة الإشارة إلى ذكر اسم المالك الأصلي لكل من الآليات الثلاثة، والتي تظهر في الشكل (3-27).

الاقتباس الجزئي

اقتباس مع إيجاز لجزء من الفكرة الأصلية تدعم الفكرة الحالية.

الاقتباس غير المباشر

التعبير عن فكرة الغير بإعادة صياغتها بأسلوب كاتب العمل.

الاقتباس المباشر

نقل النص كما هو بشكل حرفي مع وضعه بين علامتي تنصيص " "

شكل (3-27): آليات الاقتباس العلمي

يتضمن التوثيق (Citation) الإشارة إلى أسماء المراجع التي تمّ الرجوع إليها، والاستشهاد منها كأفكار أو اقتباسات. يوجد العديد من أنظمة التوثيق للمراجع على سبيل المثال (APA، MLA، هارفرد، وغيرها)، وسيتم التعامل في هذا الدرس بنمط (APA)، الذي ينقسم إلى: توثيق في المتن، وتوثيق في قائمة المراجع، وتشمل معلومات التوثيق في الغالب على: اسم المؤلف، سنة التأليف/النشر، اسم العمل، دولة النشر، مجلة/دار النشر. يشير الجدول (3-26) إلى طريقة توثيق الكتابات العلمية.

جدول (6-3): طريقة التوثيق بنظام APA

التوثيق في قائمة المراجع	توثيق المرجع في المتن	
	(بداية الفقرة)	(نهاية الفقرة)
عبدالله، محمد. (2009). المواطنة الرقمية في حياتنا. المملكة العربية السعودية: دار النشر والتوزيع.	أشار عبدالله (2009م)	 (عبدالله، 2009م).

نشاط فردي



24-3

حدد نوع الاقتباس الصحيح للعبارات من بين أنواع الاقتباسات الموجودة في الجدول الآتي:

م	النص الأصلي	النص المقتبس	نوع الاقتباس
1	لايونز، 2012: أحد الأهداف الأساسية لمنهج المواطنة الرقمية هو تعزيز السلوك الأخلاقي على الإنترنت وتقليل السلوك المحفوف بالمخاطر، والذي غالباً ما يتطلب تغييراً في السلوك.	وبيّن لايونز (2012) كذلك بأن تعزيز السلوك الأخلاقي وتحجيم السلوك المحفوف بالمخاطر من أهم أهداف منهج المواطنة الرقمية.	☐ الاقتباس المباشر.
			☐ الاقتباس غير المباشر.
			☐ الاقتباس الجزئي.
2	قال الإمام الحسن البصري في حفظ اللسان: «لِسَانُكَ سَيْفٌ قَاطِعٌ يَبْدَأُ بِكَ، وَكَلَامُكَ سَهْمٌ نَافِذٌ يَرْجِعُ عَلَيْكَ»، لذلك حلي بالمسلم أن ينتبه إلى ما يقوله.	وكما ذكر الإمام الحسن البصري عن حفظ اللسان بأن «لِسَانُكَ سَيْفٌ قَاطِعٌ يَبْدَأُ بِكَ، وَكَلَامُكَ سَهْمٌ نَافِذٌ يَرْجِعُ عَلَيْكَ»، لذلك حلي بالمسلم أن ينتبه إلى ما يقوله.	☐ الاقتباس المباشر.
			☐ الاقتباس غير المباشر.
			☐ الاقتباس الجزئي.

نشاط



حدد نوع التوثيق في كل من الأمثلة الآتية:

م	المثال	نوع التوثيق (في المتن/قائمة المراجع)
1	وذكر (ابن القيم، 1350م) (إن أعمال البر تنهض بالعبد، وتقوم به، وتصعد إلى الله به).	
2	على المواطن الرقمي إظهار معايير السلوك، والجمع بين المهارات، والمعرفة، والمواقف الرقمية، من أجل المشاركة في المجتمع كمتعلم نشط ومتصل مدى الحياة (Netsafe, 2016).	
3	رييل، مايك. (2013). تنشئة الطفل الرقمي- دليل المواطنة الرقمية لأولياء الأمور. (مكتب التربية العربية لدول الخليج، مترجم). الرياض، المملكة العربية السعودية: مكتب التربية العربية لدول الخليج (2009).	

تدريب فردي



طبق آليات الاقتباس الثلاثة كما في شكل (3-28) على النص الآتي:

النص الأصلي:

من أقوال خادم الحرمين الشريفين الملك سلمان بن عبد العزيز آل سعود-حفظه الله:-
هدفي الأول أن تكون بلادنا نموذجًا ناجحًا ورائدًا في العالم على كافة الأصعدة، وسأعمل معكم على تحقيق ذلك

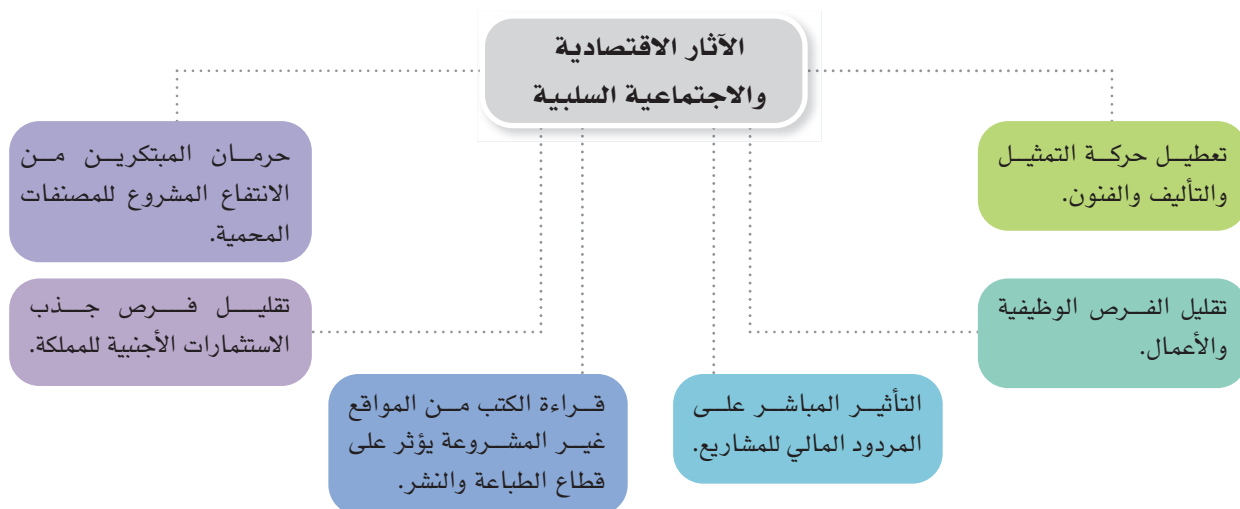
الاقتباس المباشر:

الاقتباس غير المباشر:

الاقتباس الجزئي:



الآثار الاقتصادية والاجتماعية السلبية لانتهاكات المواقع الإلكترونية للمصنفات الأدبية والفنية



شكل (28-3): الآثار الاقتصادية والاجتماعية السلبية لانتهاك حماية حقوق الملكية الرقمية

نشاط فردي



26-3

بعد معرفتك للآثار الاقتصادية والاجتماعية السلبية لانتهاك حماية حقوق الملكية الفكرية، استنتج الفوائد الإيجابية في تطبيق أنظمة حقوق الملكية الفكرية على نمو الاقتصاد الوطني.

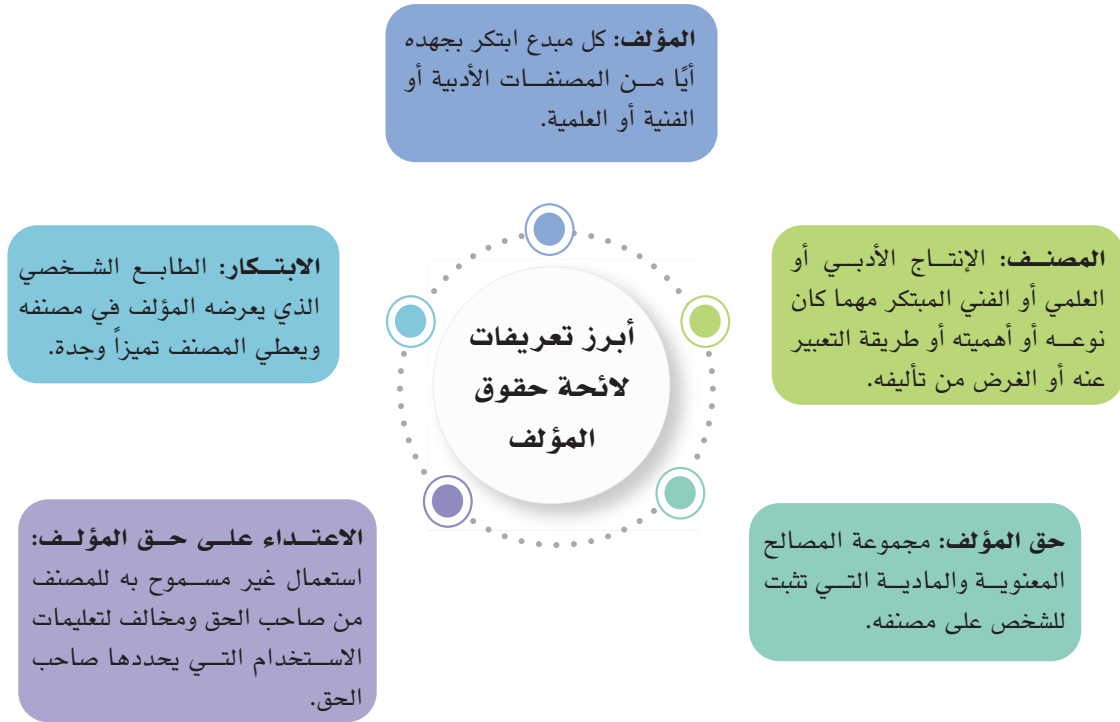


نظام حماية حقوق المؤلف السعودي

أقرّ مجلس إدارة الهيئة السعودية للملكية الفكرية بتاريخ 1443/11/17هـ تعديلات على نظام حماية حقوق المؤلف المقرر من قبل مجلس الوزراء بالمملكة العربية السعودية سابقاً، وتعد حقوق المؤلف من المجالات الإبداعية للملكية الفكرية، ويسعى النظام لحفظ حقوق المؤلف الأدبية والمادية كاملة، وتمنح المؤلف الحق في استعمال واستغلال العمل، ومنع الآخرين من استعماله أو الانتفاع به دون موافقة صاحبه الأصلي.

تتكون اللائحة من أربعة أبواب، متضمنة اثنان وخمسون مادة تختص بتعريف وحماية وتنظيم وإصدار مخالفات على مصنفات المؤلفين. وفيما يلي عرض لبعض مواد اللائحة التي تهم المواطن الرقمي:

المادة الأولى: أبرز التعريفات التي تعرضها اللائحة:



شكل (29-3): أبرز تعريفات لائحة حقوق المؤلف



المادة الحادية عشرة: مسؤولية الاعتداء

- **أولاً:** يعتبر معتدياً على حق المؤلف كل من يقوم بأي من المخالفات الواردة في النظام.
- **ثانياً:** تعتبر المنشآت مسؤولة عن أي مخالفات يرتكبها أحد العاملين بها على أي مصنف فكري إذا ثبت علمها أو تقصيرها، مثل الاحتفاظ ببرامج حاسب أو أشرطة مسموعة أو مرئية مزورة أو منسوخة، أو إجراء صيانة لجهاز إلكتروني محمل ببرامج مزورة أو مفككة الشفرة أو نحو ذلك من مصنفات.
- **ثالثاً:** يعتبر تعدياً على حقوق المؤلف ومخالفًا لأحكام النظام وهذه اللائحة، كل من أعاد إنتاج مصنفات محمية أو باع هذه المصنفات أو استوردها أو صدرها أو تولى نقلها أو نشرها أو تأجيرها.

المادة الثانية عشرة: التعدي على المصنفات الأدبية

- **أولاً:** يعتبر في نطاق الاستخدام الشخصي كل استعمال للمصنف الفكري بقصد الاستخدام الشخصي الخاص دون سواء مثل استنساخ المصنف بغرض الاحتفاظ بالنسخة الأصلية والكتابة على النسخة المستنسخة أو لترجمة فقرات منه أو لكتابة تعليقات تعبر عن الرأي الشخصي وما تعدى هذه الأغراض اعتبر تجاوزاً لحدود الاستخدام الشخصي.
- **ثانياً:** يعتبر تعدياً كل استخدام للمصنف يتخطى مفهوم الاستخدام الشخصي في مثل الحالات الآتية:
 1. استخدام ونسخ المصنف أو الاستعانة به واستغلاله لأداء مهام وظيفية.
 2. استخدام المصنف لأغراض تجارية أو استهداف الربح.
 3. استخدام المصنف بوجه مغاير عن أوجه الاستخدامات المشروعة التي نص عليها النظام.
 4. تأجير المصنف أو استنساخه أو السماح لآخرين باستنساخه أو تحويله بحجة امتلاك نسخة أصلية.
 5. أي تصرفات تعيق المؤلف من ممارسة حقه الأدبي أو المالي.
- **ثالثاً:** كما يفهم من البند ثانياً من المادة التاسعة من النظام فإن الحقوق المالية تتضمن حق الاستنساخ بأي قصد أو شكل بما في ذلك الاستنساخ الرقمي.
- **رابعاً:** يعد تعدياً على حق المؤلف استنساخ المصنف بقصد توفير نسخ منه للاستغلال التجاري أو لبيعه على طلبه العلم أو المؤسسات التعليمية أو غير ذلك.
- **خامساً:** امتلاك صاحب العمل لنسخة أصلية من المصنف، لا يعطيه حق استنساخها وتوزيعها على موظفي منشأته بحجة أنها استخدام شخصي.



المادة الثالثة عشرة: التعدي على المصنفات السمعية والبصرية وال بث الإذاعي

- يعتبر تعدياً على حق المؤلف في المصنفات السمعية والمرئية والإذاعية عند تجاوز طرق الاستخدام التي حددها من يملك حقها ومن أمثلة ذلك ما يلي:
- 1. إذاعة المصنف للجمهور دون الحصول على ترخيص مسبق من أصحاب الحق، مثل استخدام الإذاعة أو الموسيقى أو الفيديو أو البث الفضائي في المحلات التجارية والمطاعم والفنادق والأندية والمستشفيات ونحوها من الأماكن التي يكون فيها مرتادون أو تجمعات بشرية.
- 2. كسر الحواجز الاحترازية بغرض عرض المواد الإذاعية بطرق غير نظامية.
- 3. استنساخ المواد المذاعة بغرض عرضها أو تأجيرها أو بيعها.
- 4. إضافة أو إزالة شرائح إلكترونية لأجهزة العرض بهدف تجاوز إمكانيات الحدود التي صنع بها بغرض التعدي على حقوق الآخرين.

المادة السادسة عشرة: الاعتداء على برامج الحاسب الآلي

- أولاً: تتمتع بالحماية برامج الحاسب الآلي وبرامج ألعاب الحاسب، سواء كانت بلغة المصدر أو بلغة الآلة باعتبارها أعمالاً أدبية.
- ثانياً: يعتبر تعدياً على حق المؤلف كل استخدام للبرامج يخالف الاستخدامات التي يحددها صاحب الحق مثل:
- 1. استنساخ البرامج وبرامج الألعاب.
- 2. تأجير البرامج أو برامج الألعاب أو الترخيص بالاستخدام الجماعي لها بدون وجود وثائق تخول المؤجر بممارسة هذا الحق.
- 3. تحميل الشبكات الداخلية أو الأجهزة ببرامج مستنسخة.

المادة السابعة عشرة: مسؤولية محلات الصيانة

- تعتبر المنشآت المختصة في تقديم خدمات الصيانة لأجهزة العرض والاستقبال الإلكترونية مسؤولة ومعتدية على حق المؤلف عند ضبط أجهزة لديها مفكوكة الشفرة أو محملة ببرامج مزورة أو تستخدم في أعمال الصيانة برامج مزورة.



المادة الخامسة والعشرون: الاعتداء على المصنفات الإلكترونية

- **أولاً:** يعتبر معتدياً على حق المؤلف كل من ثبت قيامه عبر المواقع الإلكترونية في شبكة الإنترنت العالمية بأي من المخالفات الواردة في النظام.
- **ثانياً:** تقع على المواقع الإلكترونية في شبكة الإنترنت العالمية مسؤولية الاعتداء على حق المؤلف وفق المحتوى الداخلي للموقع، أو ما يبيث من خلاله أو ما يرتبط عن طريقه برابط خارجي لموقع آخر تابع له في حالة ثبوت احتوائه على أي من المخالفات المنصوص عليها في النظام.



إثراء



يمكنك استعراض باقي لائحة «نظام حماية حقوق المؤلف ولائحته التنفيذية» كاملة عبر مسح رمز

الاستجابة السريع:



بناءً على اطلاعك على مواد نظام حقوق المؤلف أعلاه، حدد مدى وقوع الممارسات الرقمية في الجدول أدناه ضمن مخالفات نظام حقوق المؤلف من عدمه.

م	الممارسات الرقمية	مخالفات نظام حقوق المؤلف	
		تنطبق عليها	لا تنطبق عليها
1	قرصنة برامج الحاسوب للاستخدام الشخصي أو التجاري.		
2	الاستفادة من الصور التي لا يوجد لها حقوق في أحد تصاميمك.		
3	تضمين مقطع صوتي جاهز في إعلان خاص بك دون أخذ إذن صاحبه.		
4	الاستفادة من صورة موجودة في أحد مواقع الإنترنت.		
5	نسخ ولصق الأخبار اليومية من أحد حسابات التواصل الاجتماعي.		
6	تسمية اسم مدونتك الشخصية باسم إحدى مواقع شبكة الإنترنت.		
7	تحميل مقطع مرئي من شبكة اليوتيوب محفوظ الحقوق والتعديل عليه.		
8	تصميم فكرة تطبيق هاتف ذكي مشابه لتطبيق مشهور.		
9	الاستفادة من قصيدة شعرية من أحد المواقع مع الاستئذان من صاحبها.		
10	بث مباريات مشفرة على إحدى المواقع الإلكترونية.		
11	النسخ واللصق للمصنّفات العلمية دون الإشارة لصاحبها أو استئذانه خطياً.		



ابحث عن ممارسات رقمية خالفت حقوق الملكية الفكرية الرقمية في محيطك المدرسي أو عبر شبكة الإنترنت، مع تحديد المادة التي تنطبق عليها من نظام حقوق المؤلف.

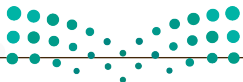
م	الممارسات المخالفة	المادة التي تنطبق عليها
1		
2		
3		

غذاء الفكر

- تأمل في ظل عدم وجود نظام ملكية فكرية يحمي الابتكارات والاختراعات، ما الحافز الذي يدفع الإنسان للتقدم والإنتاج.
- ما الحاجة لتضامن منظمات حقوق الملكية الفكرية على مستوى العالم تحت مظلة واحدة وهي منظمة (WIPO).

نقاط مهمة

- تأكد أن في حفظ حقوق الملكية الفكرية دليلاً لارتقاء المجتمعات، وتطويراً للاقتصاد المعرفي والصناعي.
- تجنبك انتحال أعمال الآخرين يحميك من التعرض للمساءلة القانونية محلياً أو دولياً.
- احرص أثناء توثيق عملك لرفعه على شبكة الإنترنت على وجود تاريخ يظهر بشكل واضح ليساعدك في حفظ حقوق الملكية الفكرية لأعمالك.
- يمكنك معاهدة التعاون بشأن براءات الاختراع في منظمات (WIPO) إمكانية تسجيل براءة اختراع واحدة لمنتجك وتكون محمية في عدد كبير من الدول بشكل متزامن.



مشروع الدرس



لما لحماية الملكية الفكرية في العصر الرقمي من أهمية كبيرة تسهم في تقدم المجتمعات حاضراً ومستقبلاً،
ساهم في تقديم توعية مجتمعية كمواطن رقمي عبر تنفيذ المشروع الآتي:
المهمة الأولى:

■ **الموضوع:** إعداد تقرير مختصر عن أهمية حفظ الملكية الفكرية في تقدم المجتمعات.

■ **الهدف:** توعية مجتمعية.

■ **عناصر الموضوع:**

- تعريف الملكية الفكرية.
- فوائد حماية حقوق الملكية الفكرية.
- أضرار انتهاك حقوق الملكية الفكرية على المجتمعات.
- نبذة عن القوانين التابعة للملكية الفكرية في المملكة العربية السعودية.

■ **موقع التنفيذ:** مدونة الطالب الشخصية.

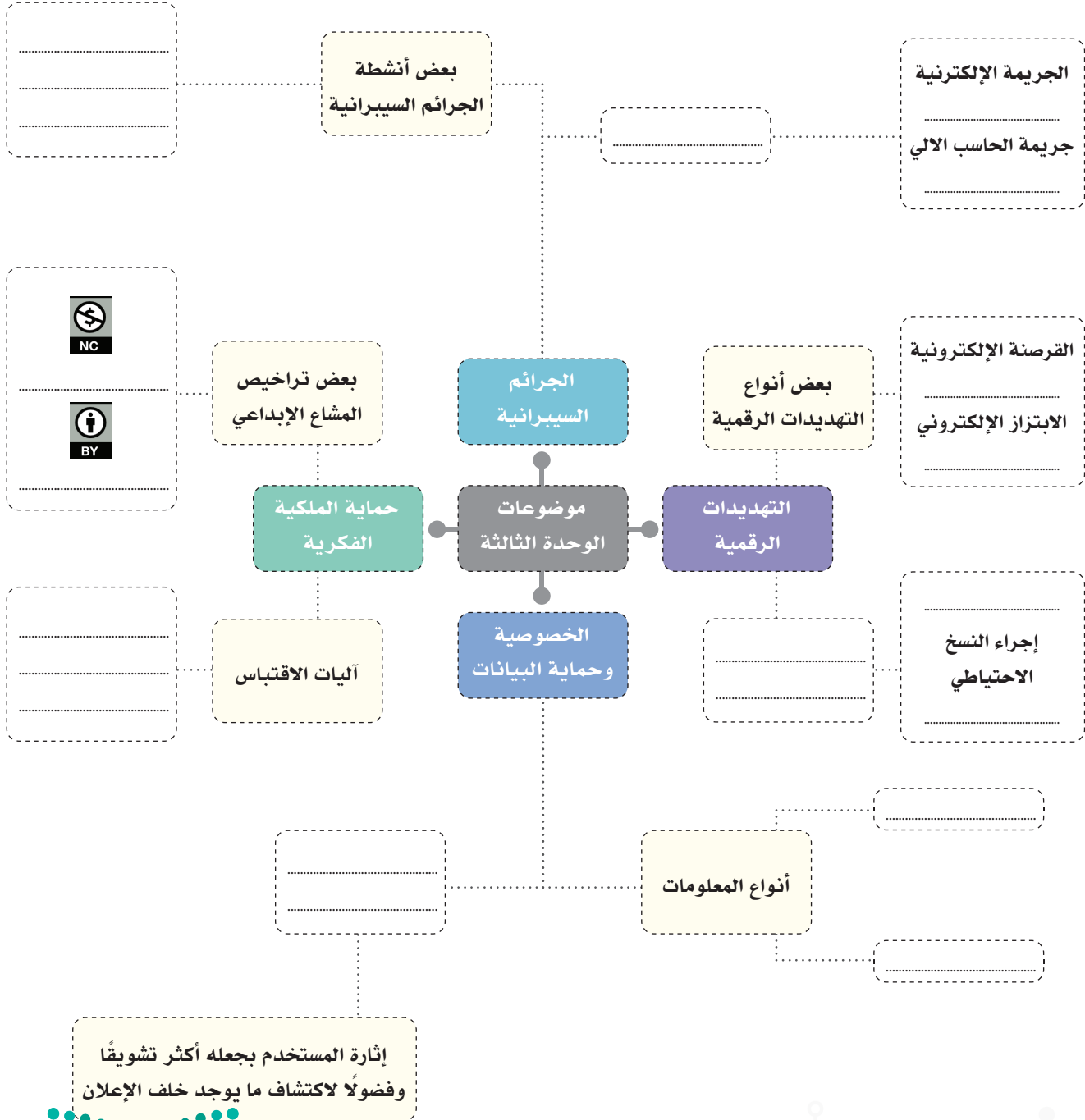
■ **خطوات التنفيذ:**

- حجز مدونة شخصية للطالب (يمكنك الاستعانة بمدونات مجانية كمدونات قوقل أو مدونات وورد برس).
- لا يقل حجم العمل عن 25 سطراً.
- توثيق أسماء المراجع داخل المتن (فقرات الموضوع).
- توثيق جميع أسماء المراجع المستخدمة في التقرير بنهاية العمل.
- توثيق أسماء مصادر الصور والأشكال تحت كل منها مباشرة.
- نشر رابط المدونة في حساباتك في وسائل التواصل الاجتماعي.



خريطة مفاهيم الوحدة

أكمل الخريطة المفاهيمية الآتية:



تقويم الوحدة

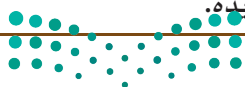
السؤال الأول: ضع إشارة (✓) أمام العبارة الصحيحة وإشارة (X) أمام العبارة الخطأ:

الإجابة	العبارة
	1. يرتكب المجرمون السيبرانيون عمليات الاختراق لمجرد التسلية والاستمتاع فقط.
	2. يكتفي المواطن الرقمي لحماية نفسه بأن يتعلم لفترة محدودة ولا يلزم الاستمرار في التعلم.
	3. كتابة كلمات المرور القوية يساعد على عدم كسرها من قبل المخترقين.
	4. ينصح بأن تكون تحديثات الأجهزة عبر شبكة الإنترنت مرة واحدة كل شهر.
	5. تتعاون قوانين مكافحة الجرائم السيبرانية في الدول للتصدي للجرائم والاستفادة من الخبرات.
	6. عدم الاهتمام بحماية معلوماتك الخاصة لا يكلفك إلا الشيء القليل من الضرر.
	7. الحرص على قراءة سياسة الخصوصية يعد كافياً للحصول على الحماية الكاملة.
	8. يساعد تطبيق نظام مكافحة جرائم المعلوماتية على حماية المصلحة العامة والأخلاق.
	9. الهدف الوحيد من استخدام طعم النقرات حث المستخدم على النقر لاختراق جهازه.
	10. المستفيد الوحيد من تجميع معلومات الأفراد من شبكة الإنترنت هم الشركات.
	11. يجب أن تشير آليات الاقتباس جميعها للكاتب الأصلي.
	12. تأثير انتهاك الملكية الفكرية يمتد للاقتصاد الوطني فقط.
	13. يغني تسجيل حقوق براءة الاختراع محلياً عن التسجيل خارجياً.
	14. يطلق مسمى الجريمة السيبرانية على أي انتهاك يحصل عبر شبكة الإنترنت.
	15. ينصح بشكل عام حفظ أرقام البطاقة البنكية في المواقع الموثوقة فقط.



السؤال الثاني: اختر الإجابة الصحيحة في كل مما يأتي:

الجملة	الخيارات
1. عملية الدخول إلى جهاز شخص آخر عبر الشبكة يعد من:	أ. القرصنة الإلكترونية. ب. الهندسة الاجتماعية. ج. التصيد الاحتيالي.
2. نوع الاقتباس الذي تُنقل به فكرة الكاتب بشكل كامل مع إعادة صياغتها هو:	أ. الاقتباس المباشر. ب. الاقتباس غير المباشر. ج. الاقتباس الجزئي.
3. أقل مراحل تنشيط المصادقة متعددة المراحل للحسابات عبر الإنترنت هي:	أ. المصادقة الثلاثية. ب. المصادقة الثنائية. ج. المصادقة الأحادية.
4. أفضل وصف لمفهوم التعقب عبر الإنترنت هو:	أ. معرفة نشاطات المستخدم عبر الإنترنت. ب. مراقبة ما يتصفحه المستخدم من مواقع الإنترنت. ج. ما يكتبه المستخدم من معلومات عند البحث في الشبكة.
5. من فوائد إجراء تحديثات أنظمة التشغيل للأجهزة باختلاف أنواعها:	أ. إغلاق الثغرات في الأنظمة لعدم اختراقها. ب. كي يكون الجهاز جديداً. ج. البحث عن الفيروسات الجديدة.



الخيارات	الجملة
أ. لا تشارك معلوماتك مع الآخرين.	6. من نصائح تحسين الخصوصية:
ب. حفظ بيانات دخول الألعاب الإلكترونية.	
ج. مشاركة موقعك على الخريطة لتسهيل الوصول.	
أ. سجن سنة وغرامة مليوني ريال.	7. عقوبة التشهير بالآخرين وفق نظام مكافحة جرائم المعلوماتية هي:
ب. سجن أربع سنوات وغرامة ثلاثة ملايين.	
ج. سجن سنة وغرامة خمسمائة ألف.	
أ. تشفير بيانات الرسالة على المرسل والمستقبل.	8. تعمل تقنية تشفير البيانات على:
ب. تشفير بيانات الرسالة على المستقبل.	
ج. تشفير بيانات الرسالة على الطرف الثالث.	
أ. RiyadhCity	9. إحدى كلمات المرور الآتية تحقق بعض إرشادات كتابة كلمة المرور القوية:
ب. Riyadh123	
ج. Riy2adh@	



أقيّم ما تعلّمت في الوحدة

- بناءً على ما تعلّمت من دروس في هذه الوحدة؛ قيّم نفسك ذاتيًا عبر معايير التقييم الموضحة في الجدول، واحسب مجموع النقاط المكتسبة.
- 2 = ينطبق بدرجة عالية.
 - 1 = ينطبق بدرجة متوسطة.
 - 0 = لا ينطبق.

النقاط المكتسبة	مقاييس التقدير			معيّار التقييم
	0	1	2	
2/.....	لم أعرف الجريمة السيبرانية، ولم أذكر أي من مصطلحاتها.	عرّفت الجريمة السيبرانية بشكل صحيح بنسبة (50%)، وذكرت اثنين من مصطلحاتها.	عرّفت الجريمة السيبرانية بشكل صحيح وبنسبة (100%)، وذكرت أربعة من مصطلحاتها.	1. تعريف الجريمة السيبرانية، وذكر مصطلحاتها الأربعة.
2/.....	لم أقترح حلول عملية لعوائق مكافحة الجريمة السيبرانية.	اقترحت من حل (1) إلى (2) حلول عملية لعوائق مكافحة الجريمة السيبرانية.	اقترحت من (3) إلى (5) حلول عملية لعوائق مكافحة الجريمة السيبرانية.	2. اقتراح حلول لعوائق مكافحة الجرائم السيبرانية.
2/.....	تصنيفي للجرائم السيبرانية الشائعة غير صحيح.	تصنيفي للجرائم السيبرانية الشائعة كان صحيحاً بنسبة (50%).	تصنيفي للجرائم السيبرانية الشائعة كان صحيحاً بنسبة (100%).	3. تصنيف الجرائم السيبرانية الشائعة في شبكة الإنترنت.
2/.....	تصنيفي للجرائم السيبرانية بحسب عقوباتها في النظام غير صحيح.	تصنيفي للجرائم السيبرانية بحسب عقوباتها في النظام صحيحاً بنسبة (50%).	تصنيفي للجرائم السيبرانية بحسب عقوباتها في النظام صحيحاً بنسبة (100%).	4. تصنيف الجرائم السيبرانية بحسب عقوباتها في نظام مكافحة جرائم المعلوماتية.
2/.....	لم أعد أي من أنواع التهديدات الرقمية الشائعة عبر الإنترنت.	عددت من (1) إلى (4) أنواع التهديدات الرقمية الشائعة عبر الإنترنت.	عددت من (5) إلى (7) أنواع التهديدات الرقمية الشائعة عبر الإنترنت.	5. تعداد التهديدات الرقمية في شبكة الإنترنت وأخطارها.
2/.....	لم أفعل أي وسيلة للحماية من خطر التهديدات الرقمية على أجهزتي.	فعلت (1) إلى (3) وسائل للحماية من خطر التهديدات الرقمية على أجهزتي.	فعلت (4) إلى (5) وسائل للحماية من خطر التهديدات الرقمية على أجهزتي.	6. تفعيل وسائل الحماية من التهديدات الرقمية باستخدام البرامج والتطبيقات.
2/.....	لم أفرق بين معلوماتي الشخصية والخاصة.	فرقت بين معلوماتي الشخصية والخاصة إلى حد ما.	فرقت بين معلوماتي الشخصية والخاصة بدرجة كبيرة جداً.	7. التفريق بين المعلومات الشخصية والخاصة أثناء استخدام شبكة الإنترنت.



أقيّم ما تعلّمت في الوحدة

النقاط المكتسبة	مقاييس التقدير			معيّار التقييم
	0	1	2	
2/.....	لم أعرف أي من أنواع المفاهيم المتعلقة بالخصوصية وحماية البيانات.	عرّفت من (1) إلى (4) مفاهيم متعلقة بالخصوصية وحماية البيانات.	عرّفت من (5) إلى (7) مفاهيم متعلقة بالخصوصية وحماية البيانات.	8. تعريف المفاهيم المتعلقة بالخصوصية وحماية البيانات.
2/.....	لم أطبق أي وسيلة لحماية الخصوصية في المواقع والتطبيقات.	طبقت من (1) إلى (3) وسائل لحماية الخصوصية في المواقع والتطبيقات.	طبقت من (4) إلى (6) وسائل لحماية الخصوصية في المواقع والتطبيقات.	9. تطبيق وسائل حماية الخصوصية وحماية البيانات في المواقع والتطبيقات.
2/.....	أنشأت كلمة مرور ضعيفة، ولم أتبع إرشادات كتابة كلمة المرور الآمنة.	أنشأت كلمة مرور متوسطة القوة ومطابقة لبعض إرشادات كتابة كلمة المرور الآمنة.	أنشأت كلمة مرور قوية ومطابقة لإرشادات كتابة كلمة المرور الآمنة.	10. إنشاء كلمات مرور قوية لحماية الخصوصية في شبكة الإنترنت.
2/.....	لم أعرف مفهوم الملكية الرقمية.	عرّفت مفهوم الملكية الرقمية بنسبة صحة (50%).	عرّفت مفهوم الملكية الرقمية بنسبة صحة (100%).	11. تعريف مفهوم الملكية الرقمية.
2/.....	لم أوثّق المراجع والبحوث، أو توثيقي لأنشطة الدرس كان خاطئاً.	وثقت المراجع والبحوث في أنشطة الدرس بنسبة صحة بلغت (50%).	وثقت المراجع والبحوث في أنشطة الدرس بنسبة صحة بلغت (100%).	12. ممارسة التوثيق الصحيح للمراجع في الأعمال.
2/.....	لم أطبق نظام حماية المؤلف في نشاط الدرس، أو تطبيقي كان خاطئاً.	طبقت نظام حماية المؤلف على بعض الممارسات الرقمية في نشاط الدرس بنسبة صحة (50%).	طبقت نظام حماية المؤلف على جميع الممارسات الرقمية في نشاط الدرس بنسبة صحة (100%).	13. تطبيق نظام حماية حقوق المؤلف على الممارسات الرقمية للحقوق الفكرية.
26/.....	المجموع			

لحساب مجموع النقاط:

- 20 فأعلى = متمكن بدرجة عالية.
- من 14 إلى 19 = متمكن إلى حدٍ ما.
- أقل من 14 = غير متمكن.



دليل مصطلحات الكتاب

المصطلح بالعربي	باللغة الإنجليزية	التعريف
الابتزاز الإلكتروني	Online Blackmail	تخويف الشخص أو تهديده بكشف معلومات خاصة أو محرجة عنه ونشرها عبر شبكة الإنترنت؛ بهدف التحكم بالشخص للقيام بأعمال غير قانونية، أو الحصول على المال، أو إجباره على فعل أمر ما يخالف الدين أو العرف المجتمعي.
آداب السلوك الرقمي	Netiquette	الأخلاقيات وقواعد السلوك للتواصل الإيجابي والفعال عبر شبكة الإنترنت لجعل العالم الرقمي مناسب للجميع.
الإدمان الرقمي	Digital Addiction	اضطراب التحكم في الانفعالات بسبب الاستخدام المفرط للأجهزة الإلكترونية والإنترنت والألعاب الإلكترونية ومنصات التواصل الاجتماعي.
اضطراب الألعاب عبر الإنترنت	Internet gaming disorder	نمط سلوكي يتميز بضعف التحكم والمشاركة المستمرة والمتكررة في الألعاب عبر الإنترنت.
الإعلام الرقمي	Digital Media	الإعلام الذي يعتمد على استخدام الإنترنت والأجهزة الإلكترونية والوسائط الرقمية لنقل المادة الإعلامية والاتصال بالجمهور، حيث يمكن إنشاء المواد الإعلامية سواء كانت مسموعة أو مرئية أو مقروءة وتعديلها ونشرها وتوزيعها من خلال التقنية الرقمية.
إعلام المواطن	Citizen media	إعلام يصنعه أو يشارك في صنعه المواطن، من خلال توظيف وسائل التقنية الرقمية من أجل صناعة المواد الإعلامية.
الإعلان الموجه	Targeted Advertising	توجيه الإعلانات للمستخدمين بناءً على المعلومات التي تم جمعها منهم.
الاقتباس	Quoting	اقتباس أفكار كاتب آخر باستخدام الكلمات أو بالأسلوب اللغوي للكاتب.
الإقصاء	Exclusion	استبعاد أو عزل شخص ما بشكل متعمد من بعض الأنشطة الجماعية عبر الإنترنت بهدف مضايقته وإزعاجه.
أمان المعلومات	Information Safety	وضع المعلومات في حالة أمان بعد حمايتها، وضمان المحافظة عليها بعدم تعرضها لأي تهديدات متوقعة في المستقبل.
الانتحال الرقمي	Digital Plagiarism	إعادة استخدام فكرة شخص آخر أثناء كتابة عمل ما، ونسبها إلى الشخص المنتحل.
انتحال الشخصية	Fraping	الدخول لحساب المتمنر عليه إما باختراقه أو من خلال معرفة كلمة السر ونشر صور مسيئة ومحتوى مؤذي.

المصطلح بالعربي	باللغة الإنجليزية	التعريف
انتحال الهوية	Identity Theft	محاولة سرقة واستخدام المعلومات الشخصية للمستخدم التي تحدد هويته، وبياناته، ومكان وجوده؛ للإضرار به، أو الاحتيال بواسطتها على الآخرين.
انتزاع الفدية	Ransomware	نوع من البرامج الضارة يعمل على قفل الملفات أو تشفيرها في جهاز المستخدم بحيث لا يمكنه استخدامها إلا بعد دفع مبلغ الفدية، ويكون الدفع عادة في شكل عملة مشفرة.
براءة الاختراع	Patent	العمل الأصلي للفرد الذي يتم تسجيله في الجهة الرسمية لحفظ الحقوق الفكرية.
البرامج الضارة	Malware	مجموعة من البرمجيات التي صممت لغرض إلحاق الضرر بأجهزة الحاسوب والمستخدمين كالفيروسات، والديدان، والأحصنة الطروادة، والتجسس.
البصمة الرقمية	Digital Footprint	أثر البيانات والمعلومات التي يتركها الشخص عند استخدام شبكة الانترنت من خلال أنشطته الرقمية المختلفة.
البيانات الضخمة	Big Data	البيانات الهائلة والمعقدة التي أتيت من خلال الرقمنة (digitization)، والتي لا يمكن معالجتها، وتحليلها من خلال التقنيات التقليدية لمعالجة البيانات.
التأنيب	Blaming	علاقة يقوم فيها أحد الأطراف بأداء دور الضحية بشكل دائم، ويحرص على أن يشعر الطرف الآخر بالذنب لكل تصرف يقوم به.
تبديل نمط لغة الحوار	Code switching	تبديل الأسلوب المستخدم في التواصل اعتماداً على مع من تتواصل أو وسيلة التواصل التي يتم استخدامها.
التجارة الإلكترونية	e-Commerce	نشاط ذو طابع اقتصادي يباشره موفر الخدمة والمستهلك بوسيلة إلكترونية من أجل بيع، أو تقديم خدمات، أو الإعلان عنها، أو تبادل البيانات الخاصة بها.
التحقير	Humiliating	تلقي شخص ما تعليقات سلبية أو انتقادات علنية عبر شبكة الإنترنت بتعمد من شخص آخر بقصد التقليل من شأنه أو التقليل من قدراته أو التقليل من إنجازاته.
ترخيص المشاع الإبداعي	Creative Commons License	منح أذونات حقوق النشر للأعمال الإبداعية من قبل ملاكها بطريقة متعارف عليها بين الجميع.
الترصد	Stalker	متابعة شخص لمستخدم آخر على جميع وسائل التواصل الاجتماعي بقصد مراقبته ومعرفة جميع تحركاته أو معرفة معلومات أكثر عنه؛ لأسباب منها مقابله في الواقع أو هوس شخصي لديه تجاه هذا الشخص أو لابتزازه أو لتهديده.
تشفير البيانات	Data Encryption	إخفاء المعلومات المهمة لتظهر بشكل غير مفهوم عند محاولة قراءتها من قبل شخص أو جهة غير مصرح لهم بالاطلاع عليها.
التشويه	Denigration	تعمد تشويه سمعة المتنمّر عليه عن طريق نشر الشائعات وإرسال معلومات خاطئة ومفبركة ونشرها عبر الإنترنت.
المضايقة	Trolling	الإساءة للآخرين عاطفياً عن طريق الإهانة والسخرية أو التقليل من شأنهم بشكل متعمد، غالباً بهدف المتعة فقط.



المصطلح بالعربي	باللغة الإنجليزية	التعريف
التصيد الاحتيالي	Phishing Scams	عملية خداع المستخدمين بإرسال رسائل بريد إلكتروني أو تصميم مواقع مزورة لسرقة كلمات المرور، وأرقام الحسابات المصرفية، أو تنزيل البرامج الضارة على الحاسوب.
التعاطف	Empathy	فهم شعور الآخر وما يفكر به قبل القيام بأي فعل أو ردة فعل أثناء التواصل الرقمي.
التعقب عبر الإنترنت	Online Tracking	التعرف على نشاطات المستخدم عبر شبكة الإنترنت، والأعمال التي يمارسها.
التنمر الإلكتروني	Cyberbullying	سلوك متعمد يهدف إلى إخافة أو استفزاز الأشخاص المستهدفين أو تشويه سمعتهم، ويحدث باستخدام التقنية الرقمية.
التواصل الرقمي	Digital Communication	تفاعلات متزامنة وغير متزامنة تحدث بين الأشخاص عبر شبكة الإنترنت، وتشمل التواصل عبر الصوت، والنص، والصورة، والفيديو، وتبادل المعلومات والملفات.
التوثيق	Citation	الإشارة إلى أسماء المراجع التي تم الرجوع إليها، والاستشهاد منها كأفكار أو اقتباسات.
الجريمة السيبرانية	Cyber Crime	نشاط إجرامي يستهدف أو يستخدم جهاز حاسوب أو شبكة حاسوبية أو جهازاً متصلاً بالشبكة بواسطة مجرمي الإنترنت.
حماية البيانات	Data Protection	هي شكل من أشكال حفظ الخصوصية التي تتعرض للانتهاكات من خدمات شبكة الإنترنت، والتي تعمل على جمع وتخزين وتحليل ومشاركة البيانات الشخصية للمستخدم.
الحوار المتحضر	Civil Discourse	الحوار المثمر الذي يسمح للناس بالاستماع إلى الآراء المختلفة والتعبير عن آرائهم بطريقة محترمة والتوصل إلى تفاهم مشترك.
الخداع	Trickery	كسب ود الشخص المستهدف وثقته حتى يشارك معلومات شخصية أو سرية، ثم يفضح المتنمّر المتنمّر عليه عن طريق كشف هذه المعلومات.
الخدمات الرقمية	Digital Services	الأعمال والخدمات التي تُقدّم بواسطة تقنيات الاتصال والمعلومات.
خطاب الكراهية عبر الإنترنت	Online Hate Speech	هجوم يحدث عبر شبكة الإنترنت يُستخدم فيه التصريح أو التلميح بعبارات ورموز عنصرية أو تحقيريه لشخص أو أشخاص بسبب انتمائهم لمجموعة معينة -قد يكون التمييز بسبب الانتماء: لعرق، أو جنس، أو دين، أو لون، أو توجه أو أحد العوامل الأخرى المحددة للهوية.
الدراما الرقمية	Digital Drama	الردود السلبية والمضايقات التي تحدث في الفضاء الرقمي عندما يستخدم الأشخاص وسائل التواصل الاجتماعي لبدء أو زيادة جدال أو شجار بين مجموعة من الأشخاص.
الذكاء الاصطناعي	Artificial Intelligence	نظام حاسوبي يمكنه محاكاة عمليات الذكاء البشري كالتعلم، والاستدلال، والتصحيح الذاتي.
السلبية	Negativity	شخص يغلب على منشوراته الشؤم والسلبية ويحاول غالباً إيجاد القبيح في كل ما يبشر.

المصطلح بالعربي	باللغة الإنجليزية	التعريف
السمعة الرقمية	Digital Reputation	الصورة الذهنية التي يبنها المتابع -أو ما يفكر به الناس ويعتقدونه - بناء على البصمة الرقمية التي يتركها مستخدم خدمات شبكة الإنترنت.
سياسة الخصوصية	Privacy policy	وثيقة قانونية يجب أن يوفرها التطبيق أو موقع الويب والتي توضح معلومات المستخدم التي يجمعونها وكيفية استخدامها.
السيطرة	Controlling	تحكم شخص في كيفية تفاعل شخص آخر عبر شبكة الإنترنت، كأن يطلب منه إلغاء متابعة شخص ما، أو حذف تعليق، أو عدم استخدام أحد وسائل التواصل.
شروط الخدمة	Terms of Service	مستند قانوني يجب أن يوفره التطبيق أو موقع الويب ويصف القواعد التي يجب على الشركة والمستخدمين الالتزام بها أثناء استخدام التطبيق أو الموقع في شبكة الإنترنت.
الصحة الرقمية والائزان الرقمي	Digital Health and Digital Wellbeing	الوصول لحياة متزنة صحية يستطيع فيها الأفراد التحكم في استخدام التقنية الرقمية واستثمار الوقت، من خلال الاستفادة من إيجابيات التقنية الرقمية مع الحد من أضرارها المحتملة.
الضغط	Pressure	قيام شخص بالضغط على آخر عبر الإنترنت لفعل شيء لا يريد القيام به أو لا يشعر بالارتياح لفعله، يشمل ذلك الضغط في طلب إرسال صور غير لائقة عبر الإنترنت أو مشاركة معلومات خاصة.
طعم النقرات	Clickbait	صورة أو عنوان رئيس يحاول جذبك للنقر عليه، ويوضع عادةً لأغراض الإعلان.
العلاقات الرقمية	Digital Relationships	العلاقات التي يتم التواصل بها عبر شبكة الإنترنت.
العنف الإلكتروني	Cyber Violence	استخدام التقنية الرقمية للتسبب بأذى جسدي أو نفسي أو مالي يستهدف الأفراد أو المنظمات أو المجتمعات.
فجوة الفضول	Curiosity Gap	رغبة الشخص في اكتشاف المعلومات المفقودة عنه.
القراءة الجانبية	Lateral Reading	تقييم مصداقية المادة الإعلامية من خلال مقارنتها بمصادر أخرى بهدف تمييز المعلومات المغلوطة من المعلومات الموثوقة سواء كانت المعلومة نصية أو مقطع مرئي أو مسموع.
القرصنة الإلكترونية	Electronic Piracy	عملية وصول غير مصرح بها إلى جهاز الحاسوب أو شبكة الإنترنت باستغلال نقاط الضعف في الأنظمة المشغلة لها.
كشف الذات	Self-disclosure	كشف الشخص أو مشاركته لمعلومات، أو صور، أو فيديوهات خاصة، أو محرجة عن نفسه أمام الآخرين.
المتجر الإلكتروني	Online Store	منصة إلكترونية يمكن عبرها بيع المنتجات الملموسة كالبضائع المادية التي نلمسها باليد، والمنتجات غير الملموسة كالخدمات الإلكترونية المتعددة كالتصميم والمونتاج وبناء المواقع والبرمجيات، وكل ماله صفة رقمية.



المصطلح بالعربي	باللغة الإنجليزية	التعريف
المخترقون	Hackers	مجموعة من الأشخاص متخصصون في عمليات الاختراق.
المطاردة الإلكترونية	Cyber stalking	مراقبة الشخص المستهدف وتتبعه إلكترونياً ومحاولة جمع كل المعلومات عنه، وقد تكون مصحوبة بمطاردة واقعية أو تمتد لتهديد المستهدف.
المعلومات الخاصة	Private Information	هوية الشخص التي ينفرد بها صاحبها دون غيره.
المعلومات الزائفة	Misinformation	المعلومات التي تحتوي على عناصر من الحقيقة، ولكنها غير دقيقة في مجملها والمنتشرة عبر الإنترنت دون هدف مقصود للتضليل أو التلاعب بالجمهور.
المعلومات الشخصية	Personal Information	معلومات الفرد التي لا تدل على هويته بشكل مباشر وقد تنطبق على أشخاص آخرين كالمعلومات العامة.
المعلومات المضللة	Disinformation	معلومات غير صحيحة يتم نشرها عمداً بهدف تضليل الجمهور أو توجيههم.
ملفات الارتباط	Cookies	ملفات نصية صغيرة مخزنة على جهاز حاسوب تتعقب ما يفعله الشخص على موقع في شبكة الإنترنت.
الملكية الفكرية	Intellectual Property	ما يمتلكه الفرد من إنتاج ابتداءً من الفكرة وما تحمله من ابتكار أو اختراع جديد، ومن ثم الوصول إلى الشكل النهائي لها.
المنصة الوطنية الموحدة	Unified National Platform	منصة رقمية متكاملة تقدم كافة الخدمات الحكومية بجودة وكفاءة عالية، عبر تجربة موحدة من خلال قنوات متعددة، تقدم الخدمات للمواطنين والمقيمين والزوار وأصحاب الأعمال التجارية.
المواطنة الرقمية	Digital Citizenship	مجموعة القواعد والضوابط والمعايير والمبادئ التي تضمن الاستخدام الأمثل والأمن والوعي للتقنية.
النزاهة الأكاديمية	Academic Integrity	الأمانة الفكرية والاستقامة العلمية في استخدام المعلومات ونقلها وتوثيقها ونشرها وإنتاج الأبحاث.
الهندسة الاجتماعية	Social Engineering	التلاعب النفسي بالمستخدم للحصول منه على أي معلومات تساعد المحتالين لإجراء أعمال احتيال أو سرقة أو انتحال هوية.
الهوية الرقمية	Digital Identity	الهوية التي يبنيها مستخدم الإنترنت بهدف التواجد والتواصل في المجتمعات الرقمية.
الوعي الإعلامي الرقمي	Digital Media Literacy	القدرة على البحث والوصول للمواد الإعلامية وتحليلها وتنظيمها وتقييمها وإعادة استخدامها أو إنتاجها، وخاصة في المواقف التي تتطلب اتخاذ قرار أو حل مشكلة أو اكتساب معرفة.

