الحماية من التهديدات الرقمية

وصف الدرس:

يهدف الدرس إلى توعية الطالب من أخطار التهديدات الرقمية الشائعة عبر شبكة الإنترنت، وكيف يتعامل معها عبر تطبيق وسائل الحماية الذاتية والبرمجيات والتطبيقات المتوفرة أثناء استخدامه شبكة الإنترنت.

أهداف التعلم:

1. أن يتعرف الطالب على الفرق بين أمن المعلومات، وأمان المعلومات.
2. أن يستشعر الطالب أهمية حماية معلوماته من التهديدات الرقمية.
3. أن يتعرف الطالب على التهديدات الرقمية الشائعة عبر شبكة الإنترنت.
4. أن ينمي الطالب وعيه بالتعامل مع التهديدات الرقمية الشائعة عبر شبكة الإنترنت.
5. أن يمارس الطالب وسائل الحماية الذاتية من التهديدات الرقمية الشائعة أثناء استخدام شبكة الإنترنت.
6. أن يستخدم الطالب البرمجيات والتطبيقات لحماية معلوماته على أجهزته المتعددة.
7. أن يشارك الطالب المجتمع بالتوعية عن أهمية الحفاظ على أمان المعلومات.

إرشادات للمعلم قبل الدرس:

- تقسّم أهداف الدرس إلى ثلاث حصص دراسية.
- يوجد في الحصتين الثانية والثالثة من الدرس تطبيقات عملية، ويفضّل التحضير لها والاستعداد المبكر بوقت كافٍ قبل الحصة الدراسية وذلك بتوفير خدمة الإنترنت، وتجهيز البرمجيات المطلوبة، وفحص الروابط المتوفرة، كما يفضّل أن يتوفر في الفصل الدراسي جهاز عرض (Data Show)، ووصلة ربط بين الأجهزة الذكية وجهاز العرض، كما يفضّل أن يكون القسم العملي في معمل المدرسة -إن توفر ذلك-.
- يمكن إنتاج أو تجهيز روابط لمقاطع مرئية لتطبيقات الدرس العملية في حالة عدم توفر التطبيق العملي في المدرسة.
- يفضّل تجهيز أوراق لأنشطة الدرس كي يتفاعل معها الطالب، ويكون مشاركًا في تعلّمه.
- التنويع في الدرس ما بين معرفي ومهاري واتجاهات وقيم، لذلك يجب أن يكون الطالب مشاركًا فاعلًا في عملية التعلُّم، وفاعلًا في أنشطة الدرس، ومطالبته بالاطلاع على الدرس قبل حضوره للصف الدراسي، وتنفيذ المهام أثناء الدرس وبعده

التمهيد في بداية الدرس:

- ابدأ الدرس بتوجيه سؤال إلى الطلبة عن أنواع أنشطة الجرائم السيبرانية التي تمت دراستها في الدرس السابق، وبيّن لهم أن الجرائم السيبرانية هي عبارة عن تهديدات خاصة تستهدف المواطن الرقمي بشكل يومي أثناء استخدامه لشبكة الإنترنت.
- أعطِ الطلبة مثالًا عن واحدة من أحدث التهديدات الرقمية التي حصلت مؤخرًا، مع بيان تفاصيل هذه الحادثة كتاريخ وقوعها، ومكانها، والمتضررين منها.
- بيّن للطالب بأن المعلومات التي لديه الآن مهمة للغاية، لكن مع تطور التقنية الرقمية المستمر، ووجود مخترقين بشكل متزايد، فإن هذه المعلومات قد لا تبقى محفوظة فقط لصاحبها، فاحتمالية تسريبها أو إتلافها واردٌ بنسبة كبيرة جدًا.
- وجّه سؤالًا للطلاب حول مدى استقطاع جزءٍ من وقتهم في محاولة تعلّم أساليب الحماية من التهديدات الرقمية، ويهدف هذا السؤال إلى شد انتباه الطلبة لأهمية تعلّمهم عبر شبكة الإنترنت واستغلال وقتهم لحماية أنفسهم.
- استعرض أسئلة التمهيد الموجودة في كتاب الطالب.

إجراءات تنفيذ الدرس:

- وضّح للطلاب بأن المعلومات المخزنة على جهازهم يجب الحفاظ عليها؛ لأنها متعلّقة بالفرد وهويته وكيانه وسمعته ومستقبله، وبيّن لهم أن المعلومات كالمال يجب المحافظة عليها؛ لأنها مطمع من قِبل الآخرين، وأن حفظ المعلومات يكون بتطبيق مفهومين: أمن المعلومات، وأمان المعلومات. وتطبيق هذين المفهومين هما محور درس التهديدات الرقمية، وأنه بعد الانتهاء من الدرس يكون الطالب قد تمّكن من معرفة الخطوات والإجراءات التي تساعده في حماية معلوماته.
- بعد شرح مفهومي أمن المعلومات، وأمان المعلومات، وجه الطلبة إلى حل الأنشطة الثلاثة الآتية:
- نشاط (3-11): اجعل الطالب يفكّر لمدة دقيقتين أيهما يطبق كمفهوم حماية للمعلومات، ويبرر سبب اختياره ذلك.

الدرس الثاني

الحماية من التهديدات الرقمية

رابط الدرس الرقمي
www.ien.edu.sa

مخرجات التعلم:

- أفرّق بين أمن المعلومات وأمان المعلومات.
- أستشعر أهمية المحافظة على معلوماتي من التهديدات الرقمية.
- أتعرف على التهديدات الرقمية الشائعة في شبكة الإنترنت.
- أنمّي وعيي بالتعامل مع التهديدات الرقمية الشائعة في شبكة الإنترنت.
- أمارس الحماية الذاتية من التهديدات الرقمية الشائعة أثناء استخدام شبكة الإنترنت.
- استخدم 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 واعيًا بهذه التهديدات، وحريصًا على الاستمرار بالتعلّم للتصدي لها في سبيل حماية معلوماته، وممتلكاته. وأن يكون مواطنًا رقميًا فاعلًا بالمساهمة بنشر التوعية والتوجيه للمجتمع الرقمي.

- هل تتحقق من اسم وعنوان الرسالة ومرسلها على بريدك الإلكتروني قبل فتحها؟
- هل تحمي حاسوبك؟ وهل تفحصه بشكل دوري لتتأكد من خلوه من الفايروسات؟
- 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 لملفاتك المهمة باستمرار وفي مكان آمن؟
- هل تعرف أحدًا 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 لتمكن المستخدم 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 11-3

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

- نشاط (3-12): اعمل عصفًا ذهنيًّا للطلاب للبحث عن المعلومات التي يتعاملون معها بشكل يومي، وسجلها على السبورة (يمكن استخدام أداة worditout الإلكترونية).
- نشاط (3-13): استقبل الإجابات من الطلبة لسرد كل الاحتمالات الممكنة، وهذا النشاط يربط بين الدرس الحالي بدرس (الجرائم المعلوماتية) السابق.

نشاط 12-3

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 13-3

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

1. .....
2. .....
3. .....
4. .....
5. .....

- استعرض للطلاب التهديدات الرقمية السبعة، مع قراءة تعريفاتها، وتحديد الفرق بينها، حيث يُخلط عادةً بين أنواع التهديدات الرقمية التي ذُكرت في الدرس.

أنواع التهديدات الرقمية (Digital Threats) الشائعة عبر شبكة الإنترنت

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

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

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

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.

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.

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

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

- خصص مدة (5) دقائق ليتمكن الطالب من محاولة ربط الممارسات السلبية بالتهديدات الرقمية الشائعة عبر شبكة الإنترنت.
- يفضّل أن يعطى الطالب التدريب في ورقة مستقلة كي يتمكن من الحل باليد، أو يعرض لهم على السبورة.
- يهدف النشاط إلى توثيق فهم الطالب للتهديدات السبعة، وربط ممارساتها السلبية.

نشاط 14-3

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 | التصيّد 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، واقناعه بأنك جديد في الشركة، وأنك لا تملك معلومات الدخول على النظام.	
6	الحصول على معلومات شخص بطريقة غير قانونية، واستخدامها في طرائق غير شرعية كالاحتيال 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 متجرٍ 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.	

184

- يهدف نموذج الحماية من التهديدات الرقمية إلى توفير طريقة الحماية الكاملة التي يبحث عنها الفرد أثناء استخدام الإنترنت.
- وضّح للطالب بأن أسلوبي: الحماية الذاتية والحماية باستخدام البرمجيات مترابطان، ولا يغني أحدهما عن الآخر، وباتباع الأسلوبين فإن الحماية تكون متكاملة أثناء استخدامه لشبكة الإنترنت.

نموذج الحماية من التهديدات الرقمية

ينبغي على المواطن الرقمي لحماية نفسه أن يكون واعيًا فطنًا، ومتعلمًا مستمرًا أثناء استخدامه تقنيات شبكة الإنترنت، وتتحقق الحماية بتطبيق نموذج الحماية المتكاملة والمكون من نوعين كما يشير إليها شكل(3-7).

شكل (3-7): نموذج الحماية الرقمية المتكاملة

- خصص مدة لا تقل عن (7) دقائق ليحل الطالب تدريب (3-3) بشكل فردي.
- اجعل الطالب يسجل نقاطه أمام كل ممارسة، ونبّه على أن تكون الاستجابة الصحيحة قيمتها (1)، وبنهاية التدريب يحصي الطالب نقاطه.
- احصِ عدد الطلبة الذين لديهم (حماية عالية، حماية متوسطة، أو يحتاجون إلى تطوير ممارساتهم في الحماية) بعد جمع نقاطهم، وإيضاح عددهم على السبورة.
- يهدف هذا التدريب إلى قياس مستوى ممارسات الطالب الآمنة أثناء استخدامه لشبكة الإنترنت، وبمقارنة مستواه مع زملائه فرصة دافعة للعمل على تطوير نفسه.

أولًا: تنمية الوعي بالحماية الذاتية من التهديدات الرقمية

تدريب 3-3

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)

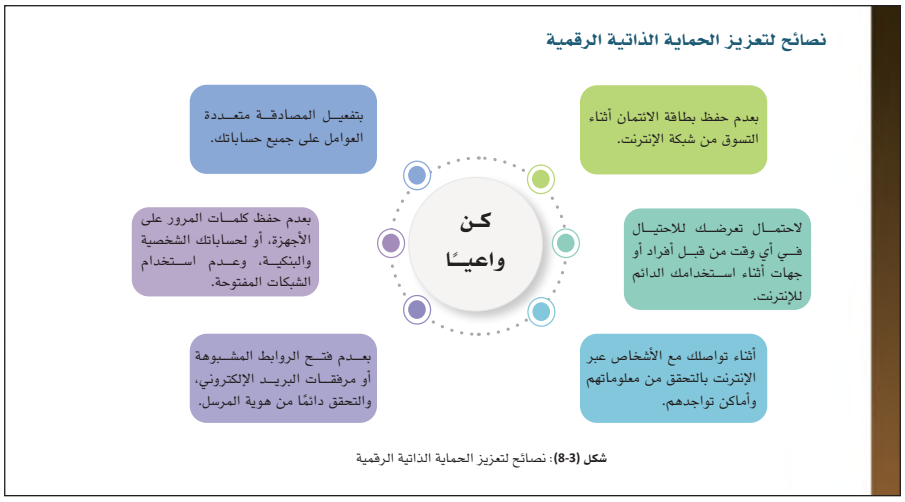
م	الممارسة الرقمية	النقاط نعم = 1 لا = صفر
1	عندما افتح رسالة بريد إلكتروني وأجد إعلانًا عن عرض مغري لمنتج، فإنني أزور موقع الشركة للتأكد من العرض، ولا أضغط على الإعلان مباشرة.	
2	عندما تصلني رسالة نصية بها رابط لتحديث بياناتي البنكية، فإنني لا أضغط مباشرة على الرابط الموجود في الرسالة إلا بعد التحقق منه.	
3	أتحقق من المعلومات والروابط المرسلة في تطبيق الواتساب من مرسلها قبل فتحها.	
4	إذا أردت زيارة موقع ما، فإنني ابحث 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	أحدّث أنظمة التشغيل مباشرة عندما يصلني تحذير بوجود ثغرات في النظام.	
11	افحص عنوان البريد الإلكتروني المرسل لي عندما ينتابني الشك في وضع الرسالة البريدية.	
12	إذا أعجبني منتجٌ ما، فإنني ابحث 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.	

- في هذا الجانب، يشاهد الطالب مقطعًا مرئيًّا عن نصائح للحماية الذاتية من التهديدات الرقمية، يفضّل أن يشاهده الطالب في المنزل قبل الحصة الدراسية، ومحاولة حل تدريب (3-3) بعد ذلك.

م	الممارسة الرقمية	النقاط نعم = 1 لا = صفر
16	لا أفتح المواقع المحجوبة لاكتشاف ما بها.	
17	لا أتجاوب 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

- تُقدَّم النصائح بعد مشاهدة المقطع المرئي، حيث إنها تعزز من وسائل الحماية للطالب في حال تعرضّه للمواقف في شبكة الإنترنت.
- يمكن عمل ورقة نشاط ليُعرف من خلالها مدى استيعاب الطالب لوسائل الحماية الذاتية من التهديدات الرقمية.



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

- يبدأ في هذا القسم الجزء العملي في الدرس، ويفضّل أن يكون الطلبة مشاركين في التطبيق العملي للدروس في معمل الحاسوب المدرسي، بالإضافة إلى توفير الوسائط المتعددة التي تخدمهم في التطبيقات المنزلية قبل الحضور للدرس وبعده.
- نبّه الطلبة بأن إنشاء كلمات المرور الآمنة والقوية والمعقدة هي أول خطوات الحماية العملية في شبكة الإنترنت، وأن الدرس القادم سيتم التفصيل في شروط وإرشادات كتابة كلمة المرور الآمنة.
- أشِر بأن إجراء النسخ الاحتياطي متوفر على كل أنظمة التشغيل والتطبيقات والبرمجيات، وأن إجراء النسخ الدوري مهم لحفظ البيانات من تلف الأجزاء المادية أو فقدانها، كما أنه حماية من تعرّض الأنظمة للأعطال المستمر.

ثانيًا: 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 تعطّل 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 (3-9): 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 (3-10): نافذة النسخ الاحتياطي لنظام تشغيل الآي أو آس

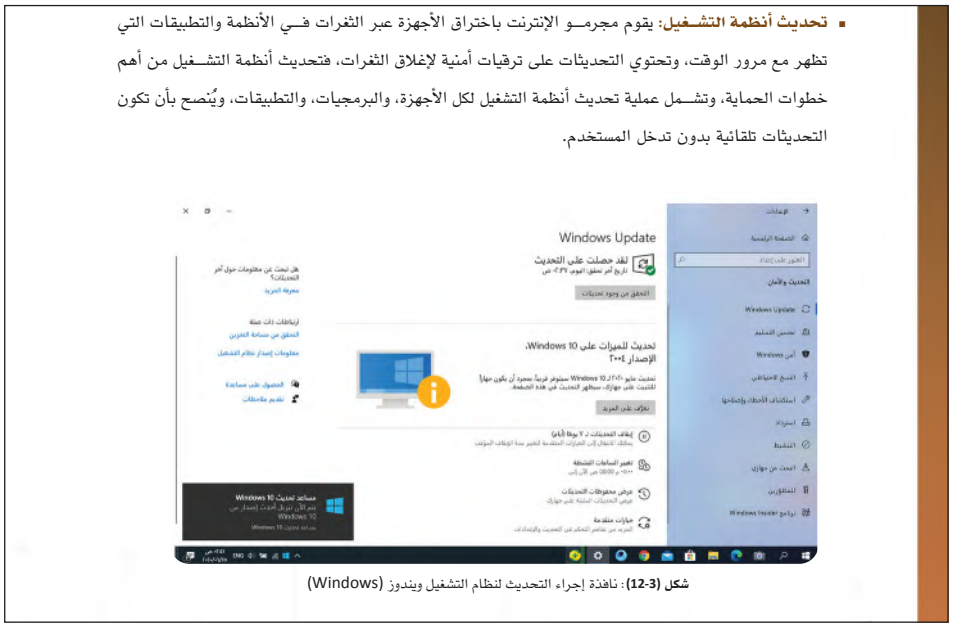
نظام تشغيل الهاتف الذكي (Android):

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

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

- في تحديث أنظمة التشـغيل قد يتعذر في بعض الأحيان إجراء الخطـوات متكاملة أمام الطلبة، يمكن الإشارة إليها عبر فتح نافذة التحديث في نظام التشغيل ويندوز (Windows).
- يمكن للطلاب إجراء التحديثات في المنزل على الأجهزة المتوفرة لديهم، ومشاركة أعمالهم عبر مدونة المادة.

- يظهر هنا الطريقة السريعة لفحص الفايروسات في نظام التشغيل ويندوز (Windows)، وتكون بالضغط بزر الفأرة الأيمن على محرك القرص الصلـب، ثم اختيار (فحص الفيروسـات)، وهي نفس الطريقة لجميع برامج مكافحة الفيروسات.
- أرشـد الطلبة بـأن برنامج مكافح الفيروسـات يعمـل فحصًـا تلقائيًا كذلـك، ويمكـن إجراء الفحـص لجهـاز الحاسـوب يدويًـا من خلال البرنامج نفسـه، وينقسم الفحص إلى: سريع أو كامل.
- فـي نشـاط (3-15) اجعل الطلبـة يبحثون عن أفضل البرمجيـات عبر مقارنتهـا ببعضها من المواقع الموثوقة، على أن تكون المقارنة حديثة في السنة الحاضرة.



- **تحديث أنظمة التشـغيل:** يقوم مجرمـو الإنترنت باختراق الأجهزة عبر الثغرات فـي الأنظمة والتطبيقات التي تظهر مع مرور الوقت، وتحتوي التحديثات على ترقيات أمنية لإغلاق الثغرات، فتحديث أنظمة التشـغيل من أهم خطوات الحماية، وتشـمل عملية تحديث أنظمة التشغيل لكل الأجهزة، والبرمجيات، والتطبيقات، ويُنصح بأن تكون التحديثات تلقائية بدون تدخل المستخدم.

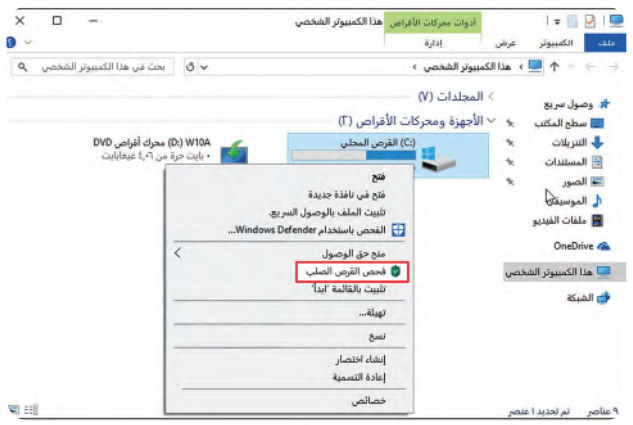
شكل (3-12): نافذة إجراء التحديث لنظام التشغيل ويندوز (Windows)

تدريب 5-3

حدّث أنظمة التشغيل التي لديك عبر تنفيذ الخطوات الآتية:

- نظام التشـغيل (Windows): من قائمة (ابدأ) اكتب في محـرك البحث (Windows Update)، واختر البرنامج من ضمن قائمة نتائج البحث انظر شـكل (3-12)، واكتب رقم نسـخة 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).

- **اسـتخدام برنامج مكافح الفايروسـات على جهاز الحاسـوب:** تكمن أهمية هذه البرامج في إجراء فحصٍ دوريٍ لكل أجزاء جهاز الحاسـوب. يمكن إجراء الفحص عبر طريقتين: إما استخدام البرمجية المتضمنة بنظام التشغيل ويندوز ذات مسمى (Microsoft Defender Antivirus)، أو بتثبيت برمجية من برمجيات الشركات التجارية، والتي يمكن اسـتخدامها بشـكل مجاني، أو بمقابل مالي، ولمعرفة طريقة فحص أقراص جهاز الحاسـوب انظر الشكل (13-3).



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

نشـاط 15-3

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

.1 .....
.2 .....
.3 .....
.4 .....
.5 .....

- وضّــح للطلاب بأن تنشــيط المصادقة متعددة العوامل يعد ضروريًّا لكل الحســابات في شبكة الإنترنت، وفي حالة عدم وجود مصادقة متعددة؛ فعلى الأقل توفير المصادقــة الثنائية التي تتم بإرســال رقم تحقق على جهاز الهاتف الذكي أو عبــر البريد الإلكتروني أثناء تســجيل الدخول إلى الحساب.
- يمكن التطرق لطريقة التحقق بالتطبيقات كما هو موجود في تطبيق نفاذ حاليًّا المستخدم في المملكة العربية الســعودية، أو بواسطة تطبيقات أخرى كما ذكر في الدرس

- **تنشــيط المصادقة متعددة العوامــل (Multi-factor Authentication):** تتضمــن الطــرق الحديثــة أثناء إنشــاء الحســابات في مواقع شــبكة الإنترنت بتفعيل المصادقــة متعــددة العوامــل (المصادقــة الثنائيــة الأكثر شــهرةً)، حيث يصعب وصــول المخترقون إلى الحسابات الشخصية، كالبريد الإلكتروني، والحسابات المصرفية، وحســابات شــبكات التواصل الاجتماعي، والدخول لأنظمة التشغيل الذكية.

يتم طلب المصادقة متعددة العوامل أثناء تسجيل الدخول لأي خدمة رقمية، وتتنوع المصادقة متعددة العوامل لأنواع عــدة: كالرســالة النصية، رســالة بالبريد الإلكتروني، رقم التعريف الشــخصي، البطاقة الذكية، بصمــة الوجه، أو تطبيق لمصادقة التحقق يتم تثبيته ســابقًا من قبل المســتخدم، ومن أمثلتها التطبيقات: (Microsoft Authenticator, Google Authenticator).

192

- وجه الطالب أثناء السير في إجراءات الدرس إلى أن يكمل جدول (3-2) بشكل دوري، وأن يحفظ الجدول في ملف الإنجاز الخاص به لاستكمال عملية التقويم في الجزء العملي.

بطاقة المواطن الرقمي للحماية من التهديدات الرقمية

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

جدول (3-2): 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	أُجري نسخًا احتياطيًا لبياناتي في أجهزتي المختلفة.				
3	أُجري تحديثًا لنظام التشغيل في جهازي.				
4	أُجري تحديثًا للبرامج والتطبيقات عندما تطلب الشركات ذلك.				
5	أفعّل التحديث التلقائي لأجهزتي.				
6	أثبّت برامج مكافحة الفايروسات في أجهزتي.				
7	أنشّط المصادقة الثنائية لحساباتي في شبكات التواصل الاجتماعي.				

حل أنشطة وتدريبات الدرس

حل نشاط (3-11): بالعودة إلى التعريفين السابقين، وضّح ما يجب عليك كمواطن رقمي التعامل معه أولًا لحماية معلوماتك الرقمية (أمن المعلومات) أم (أمان المعلومات)؟ ولماذا؟

يبدأ الطالب بأمن المعلومات قبل أمان المعلومات، حيث إن أمن المعلومات هو الحفاظ على المعلومات نفسها باتباع وسائل الحماية الذاتية وبالبرمجيات بعد أن كانت غير محمية من الأصل، وأما أمان المعلومات فهو مواصلة العمل بالحفاظ على المعلومات كتحديث البرمجيات والتطبيقات، والحذر من الدخول إلى المواقع غير الآمنة، وتجديد كلمات المرور بشكل دوري، واستخدام برامج حديثة في تخزين كلمات المرور.

نشاط (3-12) جماعي: بالتعاون مع مجموعتك، أذكر خمسة أمثلة على معلومات رقمية مهمة يجب عليك حفظها، وحمايتها لعدم تعرضها من التلف، أو السرقة، أو الاطلاع عليها من قبل الآخرين (إجابات مقترحة).

1. المعلومات الشخصية (الاسم، موقع السكن، العمر وغيرها).
2. المعلومات البنكية (أرقام الحسابات البنكية، أرقام بطاقات الائتمان، الأرقام السرية للبطاقات).
3. معلومات الحسابات (كاسم المستخدم وكلمة المرور للحسابات المهمة).
4. معلومات الدخول للأنظمة الحكومية (أبشر على سبيل المثال).

نشاط (3-13) جماعي: بالتعاون مع أفراد مجموعتك، توقع ما يمكن أن يفعله مجرمو شبكة الإنترنت أثناء حصولهم على معلوماتك الشخصية (إجابات مقترحة).

1. الوصول لملفاتك المهمة على جهازك.
2. فتح حسابات بنكية باسمك، وإجراء العمليات المالية المشبوهة.
3. الدخول على حساباتك في وسائل التواصل الاجتماعي وانتحال شخصيتك عبر التواصل مع الآخرين للقيام بتصرفات مشينة.
4. تنفيذ عمليات شراء باهظة الثمن من المتاجر العالمية.
5. مراسلة الجهات الأجنبية والمعادية للدولة.

حل نشاط (3-14): اختبر معلوماتك عن أنواع التهديدات الرقمية الشائعة عبر شبكة الإنترنت، واكتب كل مفهوم في التصنيف المناسب له:

(البرامج الضارة - الهندسة الاجتماعية - الابتـــزاز الإلكترونـــي انتـــزاع الفديـــة - التصيّد الاحتيالـــي - انتحال الهوية القرصنة)

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

سُلَّم تقدير مشروع الدرس:

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

معايير التقييم	مؤشرات الأداء	ممتاز (5)	جيد جدًا (4)	جيد (3)	مقبول (2)	ضعيف (1)
جودة وتنظيم المعلومات	المعلومات المعروضة مرتبطة بالموضوع الرئيس	المعلومات مرتبطة بالموضوع، توجد بيانات وأمثلة، واحصائيات كافية تدعم الموضوع.	المعلومات مرتبطة بالموضوع، توجد بيانات وأمثلة، واحصائيات مناسبة تدعم الموضوع.	المعلومات مرتبطة إلى حد ما بالموضوع، توجد بيانات وأمثلة، واحصائيات قليلة تدعم الموضوع.	المعلومات مرتبطة إلى حد ما بالموضوع، لا توجد بيانات وأمثلة، واحصائيات تدعم الموضوع.	المعلومات غير مرتبطة بالموضوع، لا يوجد أمثلة واحصائيات وبيانات تدعم الموضوع.
	صحة وتنظيم المعلومات في العرض	المعلومات منظمة جدًا، الفقرات مصاغة بشكل ممتاز، والأفكار متسلسلة، واستخدام العناوين الفرعية صحيح، المعلومات حقيقية.	المعلومات أقل تنظيمًا، الفقرات مصاغة بشكل جيد، والأفكار متسلسلة، واستخدام العناوين الفرعية صحيح، المعلومات حقيقية.	المعلومات شبه منظمة، الفقرات مصاغة بشكل مقبول، والأفكار شبه متسلسلة، واستخدام العناوين الفرعية شبه صحيح، المعلومات شبه حقيقية.	المعلومات شبه منظمة، الفقرات مصاغة بشكل ضعيف، والأفكار غير متسلسلة، واستخدام العناوين الفرعية شبه صحيح، المعلومات شبه حقيقية.	المعلومات غير منظمة، الفقرات ليست مصاغة بشكل سليم، وغير متسلسلة الأفكار، ولا العناوين الفرعية، والمعلومات غير حقيقية.
	الأخطاء الإملائية والنحوية والترقيم	لا يوجد أخطاء إملائية أو نحوية أو ترقيم.	أخطاء متوسطة إما إملائية أو نحوية أو ترقيم.	أخطاء إملائية أو نحوية قليلة.	أخطاء إملائية ونحوية أو ترقيم قليلة.	يوجد أخطاء كثيرة إملائية ونحوية وترقيم.
تسليم العمل	تسليم العمل للمعلم حسب الوقت	في الوقت المحدد.	تأخير أكثر من (يومين)	تأخير أكثر من (أربعة أيام)	تأخير أكثر من (ستة أيام)	تأخير أسبوع فأكثر.
مصادر المعلومات	التعدد في مصادر المعلومات	خمسة مصادر فأكثر.	أربعة مصادر.	ثلاثة مصادر.	مصدران اثنان.	مصدر واحد.
	التنوع في المصادر	قواعد البيانات، الموسوعات، محركات البحث، مواقع الهيئات والمنظمات.	قواعد البيانات، محركات البحث، مواقع الهيئات والمنظمات.	الموسوعات، محركات البحث.	محركات البحث، مواقع الهيئات والمنظمات.	محركات البحث فقط.
	توثيق المعلومات في العرض	التزام كلي بنظام التوثيق، استخدام (5) مراجع فأعلى.	التزام كبير بنظام التوثيق، استخدام (4) مراجع.	التزام متوسط بنظام التوثيق، استخدام (3) مراجع.	التزام ضعيف بنظام لتوثيق، استخدام (3) مراجع.	نظام التوثيق غير دقيق، استخدم أقل من (3) مراجع.
مواصفات العمل المطلوب	تنفيذ العدد المطلوب / المدة المطلوب	تنفيذ أكثر من المطلوب.	تنفيذ المطلوب بالضبط.	تنفيذ 70٪ من المطلوب.	تنفيذ 50٪ من المطلوب.	تنفيذ أقل من 50٪ من المطلوب.
	التقديم، الإخراج والتنسيقات، تشمل: تعدد الألوان، الوضوح، تنسيق المادة العلمية، حجم الخط المناسب، توفر مقدمة في العمل	تعدد الألوان مناسب، تنسيق جذاب، حجم خط مناسب، مقدمة تمهيدية جاذبة.	تعدد الألوان مناسب، تنسيق متوسط الجاذبية، حجم خط مناسب، مقدمة تمهيدية متوسطة الجاذبية.	تعدد الألوان مناسب، تنسيق مقبول الجاذبية، حجم خط غير مناسب، مقدمة تمهيدية متوسطة الجاذبية.	تعدد الألوان غير مناسب، تنسيق مقبول الجاذبية، حجم غير مناسب، مقدمة تمهيدية مقبولة الجاذبية.	لا يوجد تعدد للألوان، التنسيق غير جاذب، حجم خط غير واضح، لا توجد مقدمة تمهيدية.
	الإضافات في العرض	مجموعة من الرسومات والصور والجداول والزخارف.	مجموعة من الرسومات والصور والجداول.	مجموعة من الصور والجداول.	مجموعة من الصور، والرسومات.	لا يحتوي على إضافات