الوحدة 2 | الدرس 4

البصمة الرقمية وأمن الإنترنت

وصف الدرس

الغرض العام لهذا الدرس أن يستكشف الطلبة جوانب وعواقب مشاركة المعلومات الشخصية عبر الإنترنت، وأن يقوموا بتحديد المعلومات الشخصية التي لا ينبغي أن تكون عامة، وكيفية حماية هوياتهم وآثارهم الرقمية. كذلك يتوجب عليهم تمييز التدابير التي عليهم اتخاذها لحماية المعلومات الشخصية وسجلات تصفحهم للإنترنت.

ما سيتعلمه الطالب

> المقصود بالبصمة الرقمية والتعقب الرقمي.

> أنواع البيانات المسجلة أثناء استخدام الإنترنت.

> كيف يتم مشاركة المعلومات الخاصة والمخاطر المتعلقة بذلك وكيفية الحد من أضرارها.

> كيفية تصفح الشبكات الاجتماعية بشكل آمن.

> ما هي البيانات التي يحتفظ بها متصفح الإنترنت أثناء القيام بنشاطات عبر الشبكة ؟

> كيفية التعامل مع البيانات التي يخزنها متصفح الإنترنت.

> كيفية حظر النوافذ المنبثقة **Pop-up Windows**.

> تمكين برنامج **Windows Defender SmartScreen** لإيقاف المواقع المشبوهة.

> استخدام محرك البحث أو مواقع التواصل الاجتماعي للبحث عن المعلومات الشخصية لشخص ما.

> تحديد المعلومات الشخصية الخاصة التي يجب الحفاظ عليها من المشاركة والتي قد ينشأ عن نشرها مشاكل في المستقبل.

نتاجات التعلم

> آثار البصمة الرقمية للأشخاص عبر الإنترنت.
> مصادر المعلومات الشخصية وتبعات تداولها عبر الشبكة.
> ضوابط التصفح الآمن لشبكات التواصل الاجتماعي.
> استخدام وظائف نظام التشغيل لتصفح ويب آمن.
> كيفية استخدام محرك البحث للعثور على المعلومات الشخصية عبر الإنترنت.

المصطلحات

اللغة العربية	اللغة الإنجليزية
البصمة الرقمية	Digital footprint
الوصول إلى الإنترنت	Online access
التعقب الرقمي	Digital trace
إعدادات الخصوصية	Privacy settings
ملف تعريف الارتباط	Cookies
تاريخ التصفح	History
النوافذ المنبثقة	Pop-up windows
معلومات شخصية	Personal information
موقع التواصل الاجتماعي	Social networking site
استدامة البيانات الشخصية	Personal data persistence

التحديات المتوقعة

> قد يجد بعض الطلبة صعوبة في فهم أن جميع ما يقومون به على الإنترنت يترك أثرًا يشبه ما يسمى بالبصمات الرقمية. اشرح لهم المقصود بالبصمات الرقمية وماهيتها واستخدامها.

> قد يجد بعض الطلبة صعوبة في فهم أن ما يقومون بمشاركته على الإنترنت سوف يبقى على الإنترنت إلى الأبد. اشرح للطلبة كيف يتم ذلك وتأكد من أن الطلبة قد فهموا كيف تتم مشاركة ما يقومون بكتابته على الإنترنت، وأنه قد يُستخدم من قِبل المستخدمين الآخرين بطريقة غير مناسبة.

> قد يجد بعض الطلبة صعوبة في فهم طبيعة البيانات التي يجمعها متصفحهم أثناء تصفح الإنترنت. استخدم المخطط الموجود في كتاب الطالب واشرح كل عنصر من عناصر المخطط بالتفصيل.

> قد يجد بعض الطلبة صعوبة في فهم استحالة حظر المتصفح لجميع النوافذ المنبثقة. اشرح للطلبة أن هذا يرجع إلى أن من يقومون بإنشاء النوافذ المنبثقة عادة ما يبحثون عن طرق "لتجاوز" الحماية في كل متصفح. أخبر الطلبة بأن هناك برمجيات إضافية متاحة يمكن تثبيتها على متصفحهم لحظر نسبة أعلى من النوافذ المنبثقة من تلك التي تم حظرها في المتصفح من قبل، ولكن عليهم التحقق أولاً من تقييم ومراجعات المستخدمين لتلك البرمجيات قبل تثبيتها.

> قد يجد بعض الطلبة صعوبة في إدراك أن **Windows Defender SmartScreen** لا يُعدُّ كافيًا لحماية حواسيبهم من جميع أنواع من التهديدات. اشرح للطلبة أن هذا البرنامج لا يحمي حواسيبهم من الملفات الضارة على مواقع الشبكة الداخلية أو من مشاركة الملفات المصابة على الشبكة الداخلية، بل يمكن استخدام برامج مكافحة الفيروسات المخصصة لهذا الغرض.

> قد يواجه بعض الطلبة صعوبة في إدراك عدم صحة أو مصداقية الكثير من المعلومات الموجودة على شبكة الإنترنت. اشرح للطلبة بأن عليهم التأكد من صحة تلك المعلومات التي يعثرون عليها عند البحث على الإنترنت.

> قد يواجه بعض الطلبة صعوبة في فهم نوع المعلومات التي ينبغي عدم مشاركتها على الإنترنت وإمكانية تأثير تلك المعلومات على عملهم المستقبلي، وكذلك المخاطر التي قد يتعرضون لها عند الكشف عنها. وضِّح للطلبة ما لا يجب مشاركته على الإنترنت وتأثيره على حياتهم المهنية مستقبلًا بالإضافة للمخاطر التي قد يتعرضون لها وذلك بالاستعانة بكتاب الطالب كمرجع.

التمهيد

> مهِّد لغرض هذا الدرس بتحفيز اهتمام الطلبة في استكشاف جوانب وعواقب مشاركتهم للمعلومات الشخصية عبر الإنترنت. يمكنك البدء بطرح بعض الأسئلة على الطلبة على سبيل المثال لا الحصر:

- هل تدركون أنكم تتركون آثار تعقب معينة عند تصفحكم للإنترنت؟
- هل سمعتم بمصطلح البصمات الرقمية مسبقًا؟ ماذا يعني لكم هذا المصطلح؟
- لماذا يتم جمع البصمات الرقمية حسب اعتقادكم؟
- هل تعتقدون بأن بياناتكم يتم تسجيلها عند زيارة أحد مواقع الويب؟
- هل يجب التحقق من كيفية استخدام كل شركة لمعلوماتنا الشخصية ولمن تقدمها؟
- هل تعتقدون بأن ما تقومون بمشاركته عبر الإنترنت يتم حذفه؟
- ما الذي يتوجب عليكم القيام به لتصفح وسائل التواصل الاجتماعي بأمان؟
- هل تقوم متصفحات الانترنت بجمع بيانات التصفح الخاصة بكم على الإنترنت؟ إذا كانت الإجابة نعم، فما الذي يتم جمعه؟
- هل يمكنكم حذف المعلومات السابقة؟
- ما المقصود بالنوافذ المنبثقة ولماذا يتم استخدامها؟
- هل هناك طريقة لإيقاف النوافذ المنبثقة؟
- هل يمكن حظر جميع النوافذ المنبثقة بواسطة المتصفح؟
- هل سبق لكم استخدام برنامج **Windows Defender SmartScreen**؟ فما هي وظيفته؟
- هل تعتبر جميع المعلومات التي تعثرون عليها عبر الإنترنت عن شخص ما هي صحيحة؟
- اذكر بعض المعلومات التي يجب عدم مشاركتها على الإنترنت؟
- هل تعتقدون بأن المعلومات الشخصية المتوفرة على الإنترنت قد تتسبب بمشاكل مهنية للشخص؟
- ما أنواع المخاطر التي قد يتعرض لها الشخص إذا ما تمت مشاركة معلوماته على الإنترنت؟

> ساعد الطلبة بتطبيق معرفتهم باستخدام التعلم القائم على حل المشكلات والمهارات اللازمة لتطوير طرق حماية أنفسهم عند اتصالهم عبر الإنترنت.

التلميحات الخاصة بالتنفيذ

> ابدأ الدرس بالاستعانة بإرشادات كتاب الطالب لتشرح المقصود بالبصمات الرقمية وفئاتها والبيانات التي يتم جمعها أثناء زيارة أحد مواقع الويب.

> قم بالاستعانة بكتاب الطالب لشرح مفهوم البصمات (الآثار) الرقمية وفئاتها المختلفة.

> تابع الدرس بالاستعانة بإرشادات كتاب الطالب لتشرح للطلبة مصادر البيانات والمعلومات الشخصية ونتائج تداول هذه البيانات.

> بالاستعانة بكتاب الطالب اشرح للطلبة كيفية بقاء المعلومات التي يتم مشاركتها عبر الإنترنت إلى الأبد.

> تابع تنفيذ الدرس بشرح كيفية استخدام وسائل التواصل الاجتماعي بأمان للطلبة وبالاستعانة بكتاب الطالب كمرجع.

> وضِّح للطلبة أن متصفح الإنترنت المستخدم يقوم بجمع معلومات التصفح عبر الإنترنت. استعن بالمخطط الموجود في كتاب الطالب وتأكد من فهم الطلبة لكل ما ورد فيه.

> أثناء المتابعة بتنفيذ الدرس، وضِّح للطلبة أهم المعلومات التي يتم جمعها بواسطة المتصفح الخاص بهم، وكيف يمكنهم حذفها بالاستعانة بإرشادات كتاب الطالب.

> اشرح للطلبة مفهوم النوافذ المنبثقة وأسباب استخدامها، وكيف يمكنهم حظر معظمها من خلال إعدادات المتصفح باتباع الخطوات الموجودة في كتاب الطالب.

> بمتابعة تنفيذ الدرس، اشرح للطلبة الفائدة من **Windows Defender SmartScreen**. ووضح لهم كيف يمكن تفعيله باتباع الخطوات الموجودة في كتاب الطالب الخاصة بهذه المهارة.

> اشرح للطلبة بعد ذلك كيف يمكنهم العثور على معلومات موثوقة حول أحد مستخدمي الإنترنت، وما المعلومات الشخصية التي لا ينبغي نشرها، وكيف يمكنها أن تؤثر على المستقبل المهني للشخص. وفي النهاية قم بتوضيح المخاطر الكامنة من كشف الشخص عن معلوماته الشخصية بالاستعانة بمرجع كتاب الطالب.

استراتيجيات غلق الدرس

في نهاية الدرس تأكد من فهم الطلبة لجميع أهداف الدرس وقم بتقييم معرفتهم من خلال أسئلة على سبيل المثال لا الحصر:

> هل تستطيع أن تتذكر:

- ما هي البصمات الرقمية وما هي فئاتها؟
- ما هي البيانات التي يتم جمعها أثناء زيارتكم لأحد مواقع الويب؟
- ما هي الآثار الرقمية وما هي أنواعها؟
- ما هي مصادر البيانات والمعلومات الشخصية؟ وما المشاكل التي قد تحدث عند نشرها؟
- كيف يمكنك أن تنفذ نشاطاتك المختلفة على شبكة الإنترنت باستمرار وإلى الأبد بشكل آمن؟
- ما الذي يتوجب عليك القيام به لاستخدام وسائل التواصل الاجتماعي بأمان؟
- ما هي البيانات التي يجمعها متصفحك أثناء تصفحك للإنترنت؟
- ما هي بيانات المتصفح التي يمكنك حذفها من صندوق حوار الإعدادات؟
- ما هي النوافذ المنبثقة وكيف يمكنك منعها؟
- ما هو **Windows Defender SmartScreen** وكيف يمكنك تفعيله؟
- كيف تعثر على معلومات موثوقة عن شخص ما على الإنترنت؟
- ما هي المعلومات الشخصية التي يجب عدم نشرها على الإنترنت؟
- ما هي المشاكل التي قد يسببها نشر المعلومات الشخصية على الإنترنت عند البحث على وظيفة؟
- ما هي الأخطار التي تنشأ من عرض المعلومات الشخصية؟

> ذكّر الطلبة بالمصطلحات الهامة وكرّرها معهم.

> يمكنك الاستعانة بتدريبات الكتاب ضمن الاستراتيجيات التي ستستخدمها لغلق الدرس.

التدريبات المقترحة لغلق الدرس

يمكنك الاستعانة بالتمرين الأول من هذا الدرس ضمن الاستراتيجية الختامية لتقويم وتعزيز قدرة الطلبة على استيعاب المفاهيم الأساسية التي تعلموها في هذا الدرس.

الصف الثاني عشر | الفصل الأول | كتاب الطالب | صفحة 171

الفروق الفردية

تمارين إضافية للطلبة ذوي التحصيل المرتفع

> بعد الانتهاء من تنفيذ التمرين السادس، اطلب من الطلبة حذف كلمات المرور المحفوظة لآخر 24 ساعة، ثم تدوين الخطوات التي سيتبعونها لتفعيل **Windows Defender SmartScreen**. اطلب من الطلبة التحقق من صحة الخطوات التي قاموا بكتابتها من خلال التطبيق على حواسيبهم.

الإجابات النموذجية للتدريبات

1

ما المقصود بالبصمة الرقمية؟ اذكر بعض الأمثلة على ما يُمكن تعقبه رقميًا عبر الإنترنت.

> تحفظ البصمة الرقمية في شكل ملف يحتوي البيانات التي تخص المستخدم والتي يتم جمعها كنتيجة للتصفح والاتصالات والأعمال الأخرى التي يقوم بها ذلك الشخص عبر الإنترنت. يمكن تصنيف البصمة الرقمية إلى صنفين أساسيين: البصمات الرقمية النشطة، البصمات الرقمية المجهولة. يعتمد هذا التصنيف على طبيعة عمليات جمع المعلومات الخاصة بالمستخدم. عند استخدامنا لشبكة الإنترنت وتحميل صفحة ويب فإننا في الواقع نرسل طلبًا مدعمًا ببعض المعلومات إلى خادم مواقع الويب. يسجل الخادم نوع الطلب الذي قمنا به ويحتفظ ببعض تلك المعلومات مثل:

- عنوان بروتوكول الإنترنت (IP) الخاص بالحاسوب المرسل للطلب (مثلًا: حاسوب الزائر) والذي يسمح لمالكي موقع الويب بتحديد الموقع.
- مُعرِّف دخول (Login ID) الزائر.
- تاريخ ووقت الاتصال.
- طريقة الطلب (Request Method).
- اسم وموقع الملف المطلوب.
- حالة بروتوكول HTTP (مثلًا: تم إرسال الملف بنجاح، الملف غير موجود، وما إلى ذلك).
- حجم الملف المطلوب.
- صفحة الويب التي طلبت الاتصال (مثلًا: صفحة ويب تحتوي على رابط تشعبي عند ضغط الزائر عليه ينتقل إلى هنا).

2

وضِّح الخطوات الواجب عليك اتباعها من أجل تصفح اجتماعي آمن.

> كن حذرًا من مشاركة الكثير من المعلومات.

> الضبط الصحيح لإعدادات الخصوصية.

> تحديد التفاصيل التي يتم مشاركتها حول الوظيفة ومكان العمل.

> تحقق من شخصية الأشخاص الذين تتواصل معهم.

> كن حذرا عند القيام بوضع التعليقات وخذ حذرك من انتحال الهوية.

> انتبه من مشاركة تفاصيل حياتك الشخصية.

> تحقق من حسابك الخاص.

> معرفة حدود مكان العمل أو سياسات الاستخدام المقبولة.

> التحكم في المعلومات التي يتم مشاركتها مع مصادر خارجية.

> كن حذرا من الصداقات الزائدة.

> ما يتم مشاركته عبر الإنترنت يبقى على الإنترنت.

> تعرف على كيفية منع المتنمرين.

> قم باستخدام كلمات المرور القوية.

3

اذكر المعلومات التي يجب عليك عدم مشاركتها.

ما ننشره عبر الإنترنت يمكن رؤيته من قبل أي شخص، وتُعدُّ مشاركة المعلومات الشخصية مع الآخرين الذين لا نعرفهم شخصيًا أحد أكبر المخاطر التي نواجهها عبر الإنترنت، وقد تتضمن المعلومات الشخصية التي يتم مشاركتها:

- **العنوان.**
- **رقم الهاتف.**
- **أسماء أفراد الأسرة.**
- **نوع ورقم تسجيل السيارة.**
- **كلمات المرور.**
- **تاريخ العمل.**
- **الحالة الائتمانية.**
- **أرقام الضمان الاجتماعي.**
- **تاريخ الميلاد.**
- **أسماء المدارس.**
- **معلومات جواز السفر.**
- **معلومات رخصة القيادة.**
- **أرقام وثائق التأمين.**
- **أرقام القروض.**
- **أرقام بطاقات الائتمان / الخصومات.**
- **يعتبر الكشف عن الأرقام السرية لبطاقة البنك أو بطاقة الاعتماد PIN ومعلومات الحساب المصرفي أمرًا خطيرًا جدًا ويجب تجنبه.**

4

صف الأخطار التي قد تتعرض لها عند تسريب معلوماتك الشخصية.

إن تعرض معلوماتنا الشخصية للكشف قد يؤدي إلى مواجهة التالي:

- **رسوم احتيالية على بطاقة الائتمان.**
- **سحب أموال من الحساب المصرفي.**
- **الكشف عن معلومات مهمة (مثل أرقام الحسابات).**
- **اختراق حسابات البريد الإلكتروني.**
- **التحكم في حساب وسائل التواصل الاجتماعي الخاص من قبل شخص آخر.**
- **الكشف عن رقم الضمان الاجتماعي.**
- **قيام جهة أو شخص آخر بالاقتراض باسم الضحية.**
- **سرقة الهوية عبر الإنترنت.**

5

افتح Microsoft Edge وقم بتفعيل خيار حظر النوافذ المنبثقة، والتقط صورة للشاشة لما قمت به.

تلميح:

ذكّر الطلبة بأول خطوة وهي فتح مربع الحوار الخاص بإعدادات المتصفح.

6

افتح Microsoft Edge وامسح تاريخ التصفح وملفات تعريف الارتباط لآخر 24 ساعة، والتقط صورة للشاشة لما قمت به.

تلميح:

عند الضرورة قم بالتأكيد على الطلبة بأنه يجب عليهم تحديد عنصرين فقط لحذفهما.

7 افتح Microsoft Edge واستخدم محرك البحث للعثور على معلومات عن مؤسس شركة أمازون Jeff Bezos.

اكتب فقرة تتضمن أهم ما عثرت عليه.

_____

_____

_____

_____

_____

تلميح:

قم بالإشراف على الطلبة أثناء بحثهم عن المعلومات على الإنترنت. تأكد من قيامهم بجمع المعلومات المهمة فقط.

8 افتح Microsoft Edge واستخدم محرك بحث Google وحاول اكتشاف ما إذا كان هناك معلومات خاصة بك في شبكة الإنترنت.

تلميح:

قم بالإشراف على الطلبة أثناء بحثهم عن المعلومات عن أنفسهم على الإنترنت، وفي حالة عثورهم على معلومات خاصة كاسم مدرستهم، ناقش معهم بهدوء السبب المحتمل لوجود تلك المعلومات على الإنترنت وما الخطوات التي يجب عليهم اتباعها لتفادي هذا الأمر من الآن فصاعدًا.

نشاط المشروع

التلميحات وأفضل الممارسات

> اطلب من الطلبة كتابة المعلومات التي يجب أن تحتويها قائمة التحقق من أمن الحاسوب على الورق أولًا.

> يمكنك السماح للطلبة بإجراء نقاش بصوت منخفض حول تلك الأمور التي يعتقدون بضرورة وجودها في قوائم التحقق.

> بعد إجراء الطلبة النقاش والتفكير في القائمة، يمكنك أن تتدخل عند الضرورة لتنظيم عناصر قائمة التحقق التي قاموا بكتابتها. يمكنك أيضًا تسجيل تلك القائمة على السبورة أمام الفصل.

> راقب كيفية بحث الطلبة عن المعلومات على شبكة الإنترنت بحرص.

> اقترح على الطلبة تنسيق قائمة التحقق التي قاموا بإنشائها في **Microsoft Word** لجعلها تبدو أكثر احترافية.

> ساعد الطلبة إذا لزم الأمر في العثور على قوائمهم وطباعتها على طابعة الفصل أو طابعة المدرسة ومشاركة آرائهم مع زملائهم في الفصل.

الفروق الفردية

تمارين إضافية للطلبة ذوي التحصيل المرتفع

- قبل بدء الطلبة في البحث عن المعلومات، اطلب منهم تمكين حظر النوافذ المنبثقة في متصفح الويب المستخدم.
- اطلب منهم أيضًا تمكين برنامج مكافحة البرمجيات الضارة والتصيد **Windows Defender SmartScreen**.
- بعد انتهاء الطلبة من عملية البحث عن المعلومات وإنشاء قوائم التحقق الخاصة بهم في **Microsoft Word** وقبل إغلاق المتصفح، اطلب منهم مسح ملفات تعريف الارتباط وسجل التصفح.

الكفايات الأساسية للمنهج التعليمي الوطني لدولة قطر

- التفكير الإبداعي والتفكير الناقد
- الكفاية اللغوية
- الكفاية العددية
- التواصل
- التعاون والمشاركة
- التقصي والبحث
- حل المشكلات