تكنولوجيا المعلومات

INFORMATION TECHNOLOGY

كتاب الطالب

12

المسار التكنولوجي

الفصل الدراسي الثاني
2020–2021

النسخة التجريبية

binarylogic

الوحدة 1

binarylogic

تكنولوجيا المعلومات المستوى الثاني عشر

المسار التكنولوجي

كتاب الطالب / الفصل الدراسي الثاني 2020 - 2021

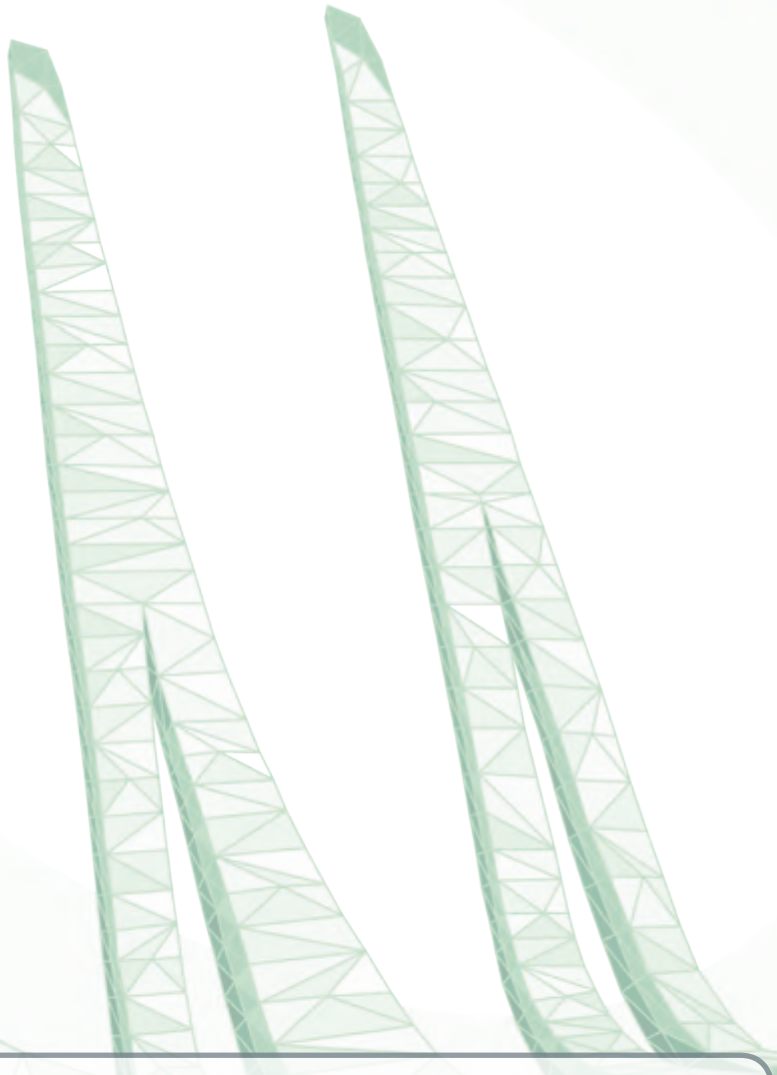
ISBN: 978-618-05-5245-4

PUBLISHED BY **MM PUBLICATIONS**

تكنولوجيا المعلومات

INFORMATION TECHNOLOGY

كتاب الطالب



الاسم .....

الشعبة .....

حضرة صاحب السمو الشيخ تميم بن حمد آل ثاني
أمير دولة قطر

النشيد الوطني

قَسَمًا بِمَنْ رَفَعَ السَّمَاءْ قَسَمًا بِمَنْ نَشَرَ الضِّيَاءْ
قَطَرٌ سَتَبْقَى حُرَّةً تَسْمُو بِرُوحِ الأَوْفِيَاءْ
سِيرُوا عَلَى نَهْجِ الأُلَى وَعَلَى ضِيَاءِ الأَنْبِيَاءْ
قَطَرٌ بِقَلْبِي سِيرَةٌ عِزٌّ وَأَمْجَادُ الإِبَاءْ
قَطَرُ الرِّجَالِ الأَوَّلِين حُمَاتُنَا يَوْمَ النِّدَاءْ
وَحَمَائِمٌ يَوْمَ السَّلاَمْ جَوَارِحٌ يَوْمَ الفِدَاءْ

مفاتيح رموز الكتاب

برامج أخرى:
قسم في نهاية الوحدة يعرض بعض الأدوات والبرامج البديلة.

المصطلحات:
قسم يوضح ما تعلمته والمفردات الجديدة التي يحتويها الدرس.

مشروع الوحدة:
نشاط في نهاية كل وحدة يدمج المهارات التي يتم تدريسها في الوحدة.

ماذا تعلمت:
قسم يركز على النقاط المهمة التي يحتاج الطلاب إلى مراجعتها.

تمرين عملي

تمرين نظري

نصيحة ذكية:
معلومات مفيدة.

كن آمنًا:
معلومات لحماية نفسك.

لمحة تاريخية:
أحداث حقيقية في الماضي.

أهلا بك!

تعال معي لنستكشف عالم تكنولوجيا المعلومات

انتقل إلى حاسوبك واتبعني!

وزارة التعليم والتعليم العالي
إدارة المناهج الدراسية ومصادر التعلم

المراجعة والتدقيق
فِرَق من:
إدارة التوجيه التربوي
الميدان التربوي

الإشراف العلمي والتربوي
إدارة المناهج الدراسية ومصادر التعلم
قسم المواد الدراسية

الكفايات الأساسية للمنهج التعليمي الوطني لدولة قطر

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

1. الأمن الرقمي

في هذه الوحدة، سيتمكن الطلبة من فهم كيفية حماية المعلومات من الوصول غير المصرح به إليها. فسيميزون أنواع المهاجمين وسيكتشفون طرقًا عدة لحماية المعلومات الشخصية. علاوة على ذلك، سيتعلم الطلبة كيفية كشف البرامج الضارة وتجنبها وسيفهمون أهمية استخدام قائمة التحقق من أمان جهاز الحاسوب. سيتعرف الطلبة على جدار النار Firewall في Windows وكيفية السماح للتطبيقات بالاتصال بالإنترنت أو حظرها. وضمن مهارات نظام تشغيل ويندوز، سيتعلم الطلبة كيفية إنشاء حسابات المستخدمين وإعداد الأذونات يدويًا لمجموعة من الملفات أو المجلدات. كما سيكون لديهم القدرة على تقييم التأثير الخاص ببصمة الشخص الرقمية عبر الإنترنت، وسيتم التعرف على استخدام وظائف نظام التشغيل من أجل التصفح الآمن للويب، والتعرف على كيفية استخدام محركات البحث عبر الإنترنت للبحث عن المعلومات الشخصية.

سيتعلم الطلبة أيضًا كيفية تبادل رسائل البريد الإلكتروني المُشفرة والموقعة رقميًا، وسيقارنون بين أنظمة التشغيل المستخدمة في الأجهزة الداعمة لإنترنت الأشياء (IoT) وأنظمة تشغيل الحواسيب المكتبية.

وأخيرًا، سيكتشفون كيف تتم عملية التجسس على حزم البيانات Packet Sniffing وسيصبحون قادرين على استخدام أداة تحليل الحزم لالتقاط الحزم واكتشاف الأنشطة المشبوهة في الشبكة.

ماذا سنتعلمْ؟

في هذه الوحِدة سنتعلم:

> ما هو أمن المعلومات ومدى أهميته.

> ما هو ثلاثي **CIA**.

> ما هي الجرائم الإلكترونية وما هي أنواعها.

> أمثلة لبعض خروقات الحماية في القرن الحادي والعشرين.

> أهم احتياطات الأمن الشخصي.

> كيفية الوقاية من البرمجيات الضارة، وكشفها وإزالتها.

> ما هو جدار النار وما هي أجياله.

> كيفية التحقق من عمل جدار النار في **Windows**.

> استخدام جدار النار في منع التطبيقات أو السماح لها بالاتصال بالإنترنت.

> حسابات المستخدمين وأنواعها في **Windows**.

> أنواع الأذونات المتاحة على الملفات والمجلدات في **Windows**.

> تعيين وتعديل الأذونات للملفات والمجلدات.

> 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 **WindowsDefenderSmartScreen** 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.

> استخدام **Microsoft Outlook** لتشفير رسائل البريد الإلكتروني وتوقيعها رقميًا.

> التعرف على الاستراتيجيات الخاصة بحماية الشبكات وتقييمها.

> المقارنة بين أنظمة تشغيل إنترنت الأشياء وأنظمة تشغيل الحاسوب المكتبي.

> ما هو التجسس على الحزم.

> ما هو محلل الحزم وما الأدوات التي تتطلبها عملية تحليل الحزم.

> استخدام برنامج **Wireshark** لاستقبال وتحليل حزم البيانات.

> كشف الأنشطة المشبوهة من خلال نتائج مسح حزم البيانات في **Wireshark**.

مواضيع الوحدة

> أمن المعلومات

> الأمن الشخصي والحاسوب

> جدار النار والحسابات والأذونات

> البصمة الرقمية وأمن الإنترنت

> أمن البريد الإلكتروني، الشبكة الخاصة الافتراضية **VPN**، وأجهزة إنترنت الأشياء **IoT**.

> التجسس على حزم البيانات **Packet Sniffing**

الأدوات

> **Microsoft Windows**

> **Microsoft Edge**

> **Google** محرك بحث

> **Microsoft Outlook**

> **Wireshark**

هل تذكر؟

تتعرض الأجهزة المتصلة بالشبكات لمخاطر متنوعة ناتجة عن البرمجيات الضارة التي تخترق أجهزة الحاسوب وتجمع البيانات المهمة وقد توقفها عن العمل، وذلك يؤثر على سلامة الشبكة بأكملها ويعرض البيانات للتلف والضياع، ويطلق على هذه البرمجيات عادة اسم "البرمجيات الخبيثة". وهي عبارة عن برامج يتم تصميمها بغرض إتلاف البيانات أو الإضرار بالأجهزة ومنعها من العمل بشكل صحيح، وتظهر بأشكال مختلفة. يتم إنشاء البرمجيات الخبيثة من قِبل أشخاص لديهم خبرة في البرمجة وشبكات الحاسوب.

يمكن أن تظهر البرمجيات الخبيثة في أشكال عديدة. البرمجيات الخبيثة هي تسمية عامة للبرامج التي تخترق أنظمة الحاسوب وتقوم بجمع البيانات المهمة من الحاسوب وقد توقفه عن العمل. أمثلة عن البرامج الضارة والخبيثة:

- أحصنة طروادة **Trojans**.
- الديدان **Worms**.
- برمجيات التجسس **Spyware**.
- البرمجيات الدعائية **Adware**.

TROJANS

WORMS

SPYWARES

ADWARES

لقد أشرنا مسبقًا إلى أن أحد تحديات شبكات التواصل الاجتماعي هي إمكانية تعرض البيانات الشخصية للسرقة. ما المقصود بالبيانات الشخصية؟ هي البيانات التي يمكن من خلالها التعرف إلى ذلك الشخص. تشمل البيانات الشخصية الاسم واسم العائلة، رقم الهاتف، و رقم الهوية الشخصية.

ينطوي التواصل عبر الإنترنت على العديد من المخاطر التي توجب عليك اتخاذ إجراءات خاصة لحماية أنفسنا، أهمها عدم ذكر اسمك أو عنوانك أو رقم هاتفك أو بياناتك الشخصية الأخرى للغرباء أو نشرها في المواقع غير المعروفة. إذا كان أحد مواقع الويب موثوقًا، فيمكنك تقديم بعض المعلومات الخاصة بك، ولكن عليك القيام بذلك بحذر دائمًا، فهناك مواقع على سبيل المثال خاصة بخدمات البريد الإلكتروني المجانية التي تتطلب إدخال الإسم و بيانات شخصية أخرى كتاريخ الميلاد. قد يلجأ البعض إلى تقديم بيانات غير حقيقية أحيانًا.

كن حذراً من الرسائل الإلكترونية التي تستلمها.

قد تحتوي الرسالة الإلكترونية على إعلانات كاذبة حول أرباح أو جوائز وهمية يمكنك الحصول عليها بالدخول إلى مواقع غير آمنة، وقد تطلب تلك المواقع إدخال معلوماتك الشخصية أو معلومات حسابك المصرفي لإرسال الجائزة المزعومة!

لذا، فإن الإفصاح عن بياناتك الشخصية قد يؤدي إلى سرقة حسابك المصرفي وسرقة هويتك ا لشخصية .

الدرس الأول

أمن المعلومات

يتعلق مفهوم الأمن الرقمي بحماية أجهزة الحاسوب والشبكات والبرامج والبيانات من الوصول غير المصرح به، والذي قد يهدف إلى الحصول على المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين، بل وأحيانًا تعطيل عمليات المؤسسة عمومًا.

أمن المعلومات

يُعبِّر مصطلح أمن المعلومات عن جميع الممارسات التي تتم لحماية المعلومات من المخاطر والهجمات التي تتمثل في الوصول غير المصرح به بغرض الاستخدام غير المشروع أو التعديل أو الإتلاف أو النسخ غير المصرح به أو تزوير المعلومات، ويمكن تلخيص اختصاصات الأمن الرقمي في النقاط الآتية:

- حماية بيانات المؤسسة وكل ما يتعلق بحفظ واستخدام تلك البيانات.
- حماية استمرارية العمل في المؤسسة.
- إتاحة التشغيل الآمن للتطبيقات المبنية على أنظمة تكنولوجيا المعلومات في المؤسسة.

أهمية أمن المعلومات

تزداد أهمية أمن المعلومات بزيادة أهمية البيانات والمعلومات المتوفرة على الشبكة، وضرورة توافرها للمستخدمين دون انقطاع، بالإضافة إلى عدد المستخدمين الذين يحتاجون للوصول إلى تلك البيانات والمعلومات بشكل مستمر، وكلما زادت أهمية المعلومات كلما كانت عرضة لهجمات القرصنة الحاسوبية بهدف سرقتها أو حجبها عن المستخدمين وغير ذلك، ...

يتمثل الدور المهم لأمن المعلومات في منع التهديدات الداخلية والخارجية واكتشافها والقيام بالاستجابة المناسبة لها حسب الضرورة.

وتُعنى إدارات تكنولوجيا المعلومات في المؤسسات المختلفة بوضع الاستراتيجية الخاصة بأمن المعلومات للمؤسسات من خلال:

أ) تحسين الوعي بقضايا أمن المعلومات من خلال التدريب والمبادرات المختلفة المتعلقة بأمن المعلومات.

ب) تحسين سياسات أمن المعلومات مع المراجعات المستمرة لتلبية متطلبات الأمان.

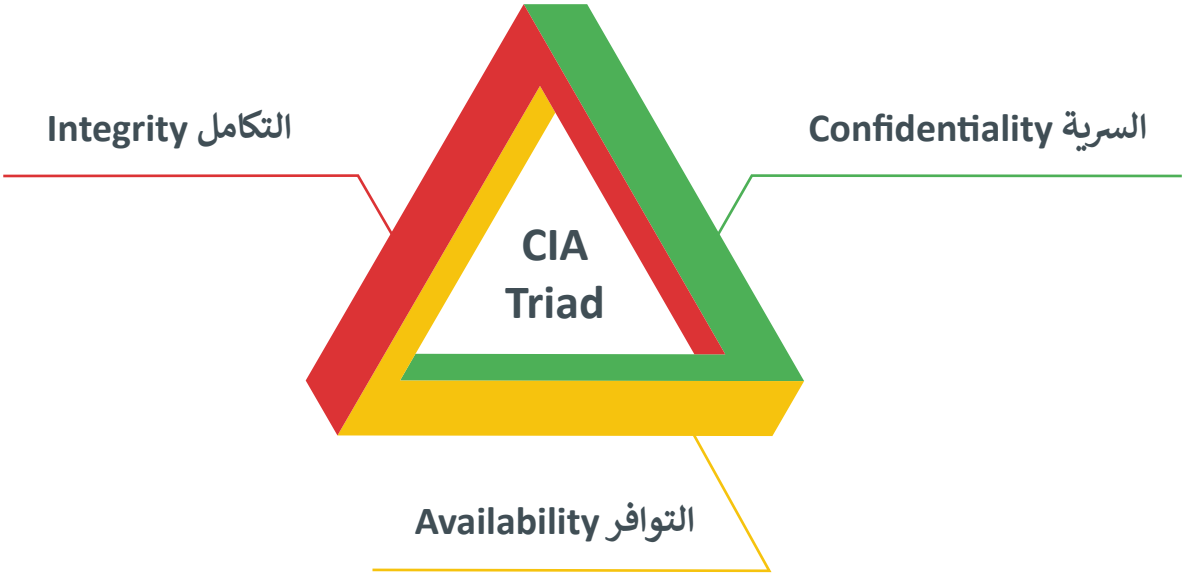
ج) تقييم التهديدات ونقاط الضعف وتحليلها بشكل دوري.

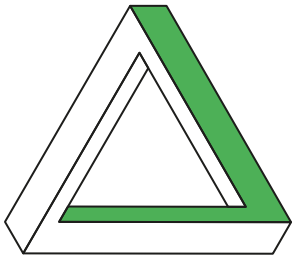
د) وضع التدابير وإجراءات الرقابة اللازمة وتنفيذها لتقليل المخاطر.

هـ) المراقبة لقياس أداء الضوابط وطرق التحكم.

مثلث الحماية CIA (CIA Triad)

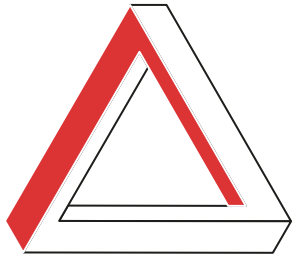
إن الهدف الأساسي لأمن المعلومات هو التركيز على توفير حماية متوازنة للبيانات من حيث سريتها وتكاملها وتوافرها (وهذا يعرف باسم مثلث **CIA**)، وذلك مع التركيز على تنفيذ سياسات أمن المعلومات بشكل فاعل وسنتعرف تفصيلًا على كل من هذه العناصر.





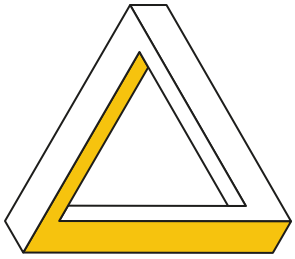
السرية Confidentiality

السرية هي إتاحة البيانات والمعلومات للأشخاص المعنيين بها فقط والمسموح لهم بالاطلاع عليها، ولتحقيق ذلك يتم استخدام أساليب مختلفة مثل اسم المستخدم وكلمة المرور، وقوائم الأشخاص ذوي الصلاحيات، وغيرها من طرق الحفاظ على سرية البيانات.



التكامل Integrity

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



التوافر Availability

التوافر يعني ضمان الوصول للمعلومات في الوقت المناسب وبطريقة موثوقة لاستخدامها، حيث أن من المُسلَّم به أن أي نظام معلومات عليه توفير المعلومات عند الحاجة إليها وذلك ليؤدي الغرض الأساسي له.

ومن أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات، الحفاظ على سلامة الأجهزة المستضيفة للبيانات، والنسخ الاحتياطي، وتحديثات النظام، وتحسين كفاءة الشبكة لتسهيل وصول المستخدمين ما أمكن.

تهدف أنظمة الجاهزية العالية (**high availability**) إلى الحفاظ على إمكانية الوصول إلى المعلومات في جميع الأوقات، كما تضمن عدم انقطاع الخدمة بسبب انقطاع التيار الكهربائي أو تعطل الأجهزة أو أثناء عمليات ترقيات النظام، وتتضمن أيضًا منع هجمات إيقاف الخدمة كتلك التي تعتمد على استهداف النظام برسائل تؤدي إلى إيقاف تشغيله إجباريًا.

الجرائم الإلكترونية Cybercrime

الجرائم الإلكترونية هي استخدام الحاسوب كأداة لتحقيق غايات غير قانونية مثل الاحتيال أو التوزيع غير القانوني للمواد المحمية بحقوق الطبع والنشر أو سرقة الهويات أو انتهاك الخصوصية.

اكتسبت جرائم الحاسوب والجرائم الالكترونية اهتمامًا متعاظمًا مؤخرا نظرًا لأن الحاسوب أصبح أداة رئيسَة للتجارة والترفيه وكذلك لأداء الأعمال الحكومية. وتختلف جرائم الإنترنت عن النشاط الإجرامي التقليدي في استخدام الأجهزة الرقمية وشبكات الحاسوب لتنفيذ تلك الجرائم. على الرغم من كون الجريمة الإلكترونية ذات طابع مختلف تمامًا عن الجريمة التقليدية إلا أنها تنفذ بواسطة نفس النوع من المجرمين ولنفس الأسباب، فمخترقو الشبكات و المتسللون هم لصوص محترفون لديهم نفس دوافع المجرمين التقليديين، حيث تتشابه الطرق التي يستخدمونها لجمع البيانات والقيام بتلك التي يتم اتباعها خلال الجرائم "التقليدية" الهادفة للسرقة، حيث يقوم المتسللون باقتحام شبكة الحاسوب لسرقة البيانات بنفس الطريقة التي يقوم بها اللصوص باقتحام بنك لسرقة الأموال.

أنواع الجرائم الإلكترونية	
الاحتيال الإلكتروني Phishing Scams	يحدث هذا الاحتيال عندما يتقمص المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية، بغرض الحصول على معلومات شخصية عن مستخدم معين مثل كلمات المرور المصرفية وعنوان البيت أو الرقم الشخصي. تتم هذه العملية عادةً من خلال مواقع الاحتيال التي تُقلد المواقع الرسمية.
سرقة الهوية Identity Theft	بعد سرقة البيانات الشخصية، يقوم المحتالون بانتحال شخصية الضحية واستخدام بياناته لإجراء معاملات مالية، أو أعمال غير قانونية.
المضايقات عبر الإنترنت Online Harassment	تشمل المضايقات عبر الإنترنت التهديدات عبر البريد الإلكتروني أو الرسائل الفورية أو المشاركات المسيئة في وسائل التواصل الاجتماعي مثل **Facebook** و **Twitter**.
التسلل الإلكتروني Cyberstalking	عادة ما يصيب المتسللون الإلكترونيون أجهزة حواسيب ضحاياهم ببرامج ضارة يمكنها تسجيل نشاط الحاسوب لمراقبة نشاطاتهم عبر الإنترنت، فمثلًا يقوم برنامج **keylogger** بتتبع وتسجيل أزرار لوحة المفاتيح المضغوطة بطريقة سرية بحيث يصعب على الشخص معرفة أنه تتم مراقبته وجمع بياناته الخاصة. من المعروف أيضًا أن المتسللين عبر الإنترنت يضايقون باستمرار ضحاياهم المحتملين أو زملاءهم وأصدقائهم لمحاولة الحصول على المعلومات الشخصية الخاصة بهم.
انتهاك الخصوصية Invasion of privacy	يحدث انتهاك الخصوصية عند محاولة شخص ما التطفل على الحياة الشخصية لشخص آخر، وقد يتضمن ذلك اختراق حاسوبه الشخصي أو قراءة رسائل البريد الإلكتروني أو مراقبة الأنشطة الشخصية الخاصة به عبر الإنترنت.

خرق الحماية Security Breach

يحدث خرق الحماية عند تجاوز طرف غير مصرح به لتدابير الحماية للوصول إلى مناطق محمية من النظام، ويمكن أن يؤدي خرق الحماية إلى سيطرة المتسللين على معلومات قيمة مثل حسابات الشركات والملكية الفكرية والمعلومات الشخصية للعملاء التي قد تشمل الأسماء والعناوين والأرقام الشخصية ومعلومات بطاقات الائتمان.

في بعض الأحيان، يتم استخدام مصطلح خرق البيانات بالتناوب مع مصطلح خرق الحماية، رغم وجود اختلاف جوهري بينهما، حيث يحدث خرق البيانات كنتيجة لحدوث خرق الحماية، كما أن اختراقات البيانات قد تحدث في مواضع مختلفة وبشكل متلاحق، حيث قد تؤدي سرقة كلمات المرور مثلًا إلى اختراق العديد من الأنظمة الأخرى عبر الإنترنت.

يميل المستخدمون عادة إلى استخدام نفس كلمة المرور على حسابات متعددة عبر الإنترنت، ورغم أنه من الصعب تذكر مجموعة من كلمات المرور المختلفة، إلا إنه من المهم جدًا استخدام كلمات مرور مختلفة لحماية البيانات في حال حدوث اختراق لأحد الأنظمة التي تستخدمها عبر الإنترنت.

Facebook

في عام 2019، كشف باحثوا أمن المعلومات أن ملايين سجلات مستخدمي **Facebook** كانت منتشرة عبر الإنترنت. قامت بعض التطبيقات التي يسمح لها **Facebook** بالوصول إلى بيانات مستخدميه وتخزينها على خوادم خاصة بها دون وضع تدابير الأمان المطلوبة. تم العثور على ملايين السجلات بما فيها معرفات المستخدمين على **Facebook**، التعليقات، الإعجابات، ردود الفعل وأسماء الحسابات في قاعدة بيانات تم تحميلها بواسطة الناشر الرقمي المكسيكي **Cultura Colectiva** الذي تم اكتشافه على خوادم السحاب **Amazon Web Service (AWS)**، وهذا يدعو إلى اتخاذ تدابير الحيطة والحذر قبل السماح لبرامج الأطراف الخارجية التي تصادفنا على منصات التواصل الاجتماعي بالوصول إلى إلى معلوماتنا.

Marriott International

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

Google+

في أكتوبر 2018، تم الإبلاغ عن خرق مبدئي طال 500 ألف من مستخدمي **Google+**، ولكن **Google** أعلنت عن الخرق بعد عدة أشهر من اكتشافه. في ديسمبر، كشفت **Google** عن خرق ثان للبيانات تم خلاله كشف المعلومات الشخصية لـ 52.5 مليون حساب على **Google+** لمدة ستة أيام لتطبيقات غير **Google+**. تضمن هذا الخرق بيانات مثل الأسماء، عناوين البريد الإلكتروني، تواريخ الميلاد ونوع المعلومات الشخصية الأخرى التي تم جمعها بواسطة **Google+**.

Twitter

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

Adobe

أعلنت الشركة في البداية بأن المتسللين سرقوا ما يقرب من 3 ملايين من سجلات بطاقات ائتمان العملاء المشفرة، بالإضافة إلى بيانات تسجيل الدخول لعدد غير محدد من حسابات المستخدمين، ولكن بعد أسابيع من البحث تم اكتشاف أن هذا الاختراق قد كشف عن الكثير من بيانات العملاء بما فيها مُعرِّفاتهم وكلمات المرور ومعلومات بطاقات الخصم وبطاقات الائتمان الخاصة بهم.

1

ضع علامة ✓ أمام العبارة الصحيحة وعلامة ✗ أمام العبارة الخطأ.

.1	يعبر مصطلح أمن المعلومات عن جميع الممارسات التي يتم تنفيذها لحماية المعلومات من المخاطر والهجمات التي تتمثل في الوصول غير المصرح به.	○
.2	يعد مثلث الحماية **CIA** (التوافر والتكامل والسرية) نموذجًا مصممًا لتوجيه السياسات الخاصة بأمن المعلومات.	○
.3	تشترك الجرائم الإلكترونية والجرائم التقليدية في دوافع الجريمة ومسبباتها، ولكنها تختلف في الوسيلة.	○
.4	يحدث خرق البيانات عندما ينتهك شخص ما التدابير الأمنية للتحكم بالمعلومات الشخصية فقط.	○
.5	لم يحدث أبداً أي خرق لبيانات **Facebook**.	○

2

وضح بالشرح العناصر التي يتكون منها النموذج الثلاثي **CIA**، ثم وضح كيفية تطبيق هذا النموذج على أنظمة الصراف الآلي **ATM**.

_____

_____

_____

_____

_____

3 طابق ما يلي:

1 الاحتيال الإلكتروني	التطفل على الحياة الشخصية للآخرين.
2 سرقة الهوية	إصابة أجهزة حواسيب الضحايا ببرامج ضارة يمكنها تسجيل نشاط الحاسوب لمراقبة نشاطهم عبر الإنترنت.
3 المضايقات عبر الإنترنت	تشمل التهديدات عبر البريد الإلكتروني أو الرسائل الفورية أو المشاركات المسيئة في وسائل التواصل الاجتماعي.
4 التسلل الإلكتروني	تتم هذه العملية عادةً من خلال مواقع الاحتيال التي تُقلد المواقع الرسمية.
5 انتهاك الخصوصية	انتحال شخصية الضحية واستخدام بياناته لإجراء معاملات مالية.

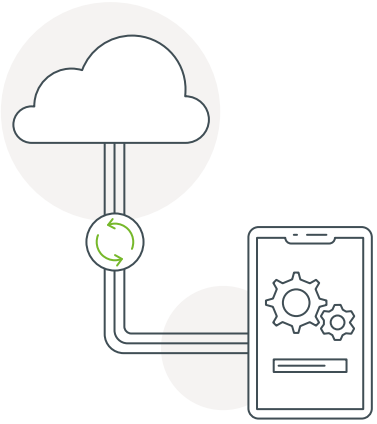
الدرس الثاني

الأمن الشخصي والحاسوب

يهدف المحتالون والمتسللون ولصوص الهوية بشكل رئيس لسرقة المعلومات الشخصية والتي من خلالها يمكنهم الاستيلاء على المال. ولتجنب مثل هذا الأمر، هناك خطوات يتعين علينا اتخاذها لحماية أنفسنا من هذه الهجمات الإلكترونية.

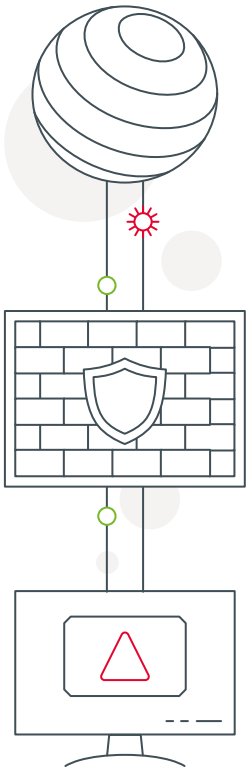
احتياطات الأمن الشخصي

تساعد حماية معلوماتك الشخصية في التقليل من خطر سرقة الهوية أو انتحال الشخصية. لا تقتصر المعلومات الشخصية على الاسم الكامل والعنوان ورقم الهاتف أو تاريخ الميلاد، بل قد تتضمن الرقم الشخصي وأرقام بطاقات الائتمان وأرقام الحسابات المصرفية والحسابات الأخرى، والتي يمكن استخدامها للسرقة أو انتحال الشخصية ... وغيرها، وفيما يلي بعض الاحتياطات التي ينصح باتخاذها للوقاية من الجرائم الإلكترونية:



التحديث الدوري للبرامج

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



استخدام مضاد الفيروسات Antivirus وجدار الحماية Firewall

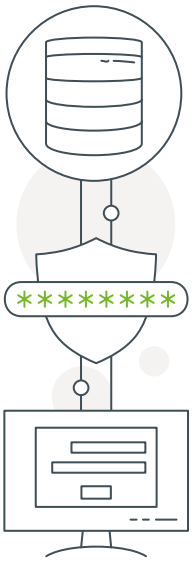
يُعدُّ برنامج الحماية من الفيروسات **Antivirus** الحل الأكثر نجاعةً في محاربة الهجمات الضارة نظرًا لأنه يمنع البرامج الضارة والفيروسات الخبيثة الأخرى من الدخول إلى جهازك وتعريض بياناتك للخطر، ويُعدُّ استخدام برنامج حماية مناسب مهمًا في الحفاظ على بياناتك من الهجمات، فهو يساعد على حجب المتسللين والفيروسات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

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

التواصل الرقمي بحذر

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

استخدام كلمات المرور القوية وأدوات إدارة كلمات المرور



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

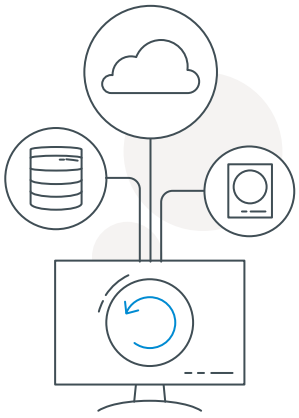
التحقق الثنائي أو المتعدد Multi-factor Authentication

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

كن حذرًا

انتبه إلى أن بعض الروابط الخبيثة قد تأتي من الأصدقاء والمعارف الذين أصيبت أجهزتهم بالبرامج الضارة دون معرفتهم.

النسخ الاحتياطي الدوري للبيانات Backup



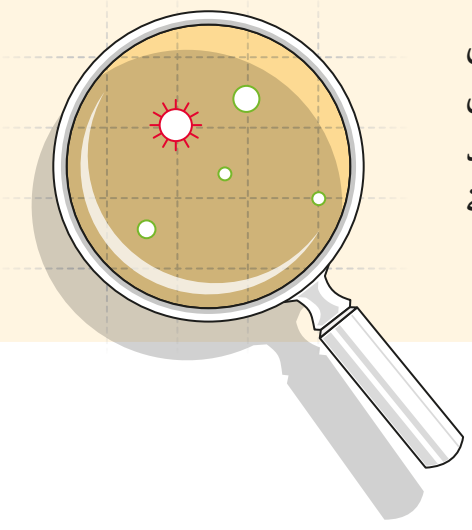
يعد إجراء نسخ احتياطي لبياناتنا بشكل دوري خطوة مهمة في مجال الحفاظ على أمن الإنترنت الشخصي، فبشكل أساسي علينا الاحتفاظ بثلاث نسخ من بياناتنا على نوعين مختلفين من وسائط تخزين البيانات، كنسختين على (القرص الصلب المحلي والخارجي)، ونسخة أخرى على موقع خارجي أو باستخدام التخزين السحابي. في حالة استهدافنا بالبرمجيات الضارة تكون الطريقة الوحيدة لاستعادة البيانات هي باستعادة آخر نسخة احتياطية كبديل عن النظام الحالي المصاب بالبرمجيات الضارة.

تجنب استخدام شبكات Wi-Fi العامة

لا يعتبر من الآمن استخدام شبكة **Wi-Fi** عامة دون استخدام شبكة افتراضية خاصة **(VPN)**، فباستخدام الشبكة الافتراضية **(VPN)**، يتم تشفير حركة نقل البيانات بين الجهاز وخادم **VPN** مما يصعب على القراصنة الوصول إلى بياناتنا على الإنترنت، كما يوصى باستخدام الشبكة الخلوية عند عدم وجود شبكة **VPN** وذلك للحصول على مستوى أعلى من الأمان.

أمن الحاسوب عبر الإنترنت

بالإضافة إلى الأمن الإلكتروني الشخصي، يجب الاهتمام أيضًا بأمن الأجهزة الحاسوبية، وذلك بحمايتها من السرقة أو التلف الذي قد يلحق بها أو بالبيانات الإلكترونية، بشكل أكثر تحديدًا، يجب حماية أنظمة الحاسوب من البرمجيات الضارة والتي تعرف باسم **Malware**.



من البرمجيات الضارة الفيروسات وبرامج التجسس التي يتم تثبيتها على جهاز الحاسوب أو الجهاز المحمول دون موافقة المستخدم أو دون معرفته، والتي قد تتسبب في تعطل الأجهزة أو استخدامها لمراقبة أنشطة المستخدمين أو التحكم بها.

تجنب البرمجيات الضارة والوقاية منها

تذكر دائمًا أن الوقاية خير من العلاج، وفيما يلي نستعرض طرقًا مختلفة لوقاية أجهزتنا من الإصابة بالبرمجيات الضارة بأنواعها.

طرق الوقاية من تحميل البرمجيات الضارة	
تثبيت وتحديث برنامج الحماية من البرمجيات الضارة، واستخدام جدار النار.	اضبط إعدادات برنامج الحماية ومتصفح الإنترنت ونظام التشغيل للتحديث تلقائيًا.
لا تقم بتغيير إعدادات أمان متصفحك.	يمكننا تقليل التنزيلات التلقائية غير المرغوب بها من خلال الاحتفاظ بإعدادات الأمان الافتراضية لمتصفحنا.
انتبه لتحذيرات الأمان الخاصة بالمتصفح.	تأتي العديد من المتصفحات مع أدوات مسح أمني مدمجة تحذرنا قبل زيارة صفحة ويب غير آمنة، أو عند تنزيل ملف ضار.
بدلاً من الضغط على ارتباط في بريد إلكتروني، اكتب عنوان URL لموقع موثوق مباشرة في المتصفح.	يرسل المجرمون رسائل بريد إلكتروني يبدو أنها من شركات نعرفها ونثق بها، وقد تبدو الروابط موثوقة، إلا أن الضغط عليها يقوم بتحميل برامج ضارة أو يرسلنا إلى موقع احتيالي.
لا تفتح المرفقات في رسائل البريد الإلكتروني إلا إذا كنت تعرف المرسل.	يمكن أن يؤدي فتح المرفق الخطأ إلى تثبيت برامج ضارة على حاسوبنا. هناك العديد من امتدادات ملفات الفيروسات مثل exe. و vbs. و cmd. و hta. و html. و scr. و msi. و msp. و pif.
احصل على البرنامج المطلوب مباشرة من المصدر.	من المرجح أن تتضمن المواقع التي تقدم خدمات تنزيل البرامج المجانية برامج ضارة.

طرق الوقاية من تحميل البرمجيات الضارة	
قراءة كل محتويات الشاشة أثناء تثبيت برنامج جديد.	أثناء تثبيت بعض البرامج على الأجهزة، قد يطلب منا تثبيت برنامج إضافي، قم برفض تنزيل هذا البرنامج أو إلغاء عملية التثبيت ككل.
لا تضغط على الإعلانات المنبثقة الخاصة بتحسين أداء الحاسوب.	يقوم المحتالون بإدراج برامج غير مرغوب فيها في إعلانات النوافذ المنبثقة والتي قد تبدو سليمة، وخاصة الإعلانات المتعلقة بتحسين قدرات الحاسوب، لذلك يجب تجنب الضغط على هذه الإعلانات في حالة عدم تعرفنا على المصدر.
افحص وحدات التخزين الخارجية قبل استخدامها.	يمكن أن تصاب وحدات التخزين الخارجية بالبرمجيات الخبيثة خاصةً إذا استخدمناها لنقل البيانات بكثافة بين الأجهزة الشخصية والعامة.
ناقش مسائل الأمان الحاسوبية مع الآخرين.	أخبر الأصدقاء والعائلة أن بعض الإجراءات عبر الإنترنت يمكن أن تعرض الحاسوب للخطر، مثل الضغط على النوافذ المنبثقة أو تنزيل ألعاب أو برامج "مجانية" أو غيرها ...
استخدم النسخ الاحتياطي لبياناتك بانتظام.	يجب علينا عمل نسخ احتياطية من أية بيانات نرغب في الاحتفاظ بها في حالة تعطل جهاز الحاسوب الخاص بنا، وبشكل خاص الصور و المستندات المهمة.

الكشف عن البرامج الضارة

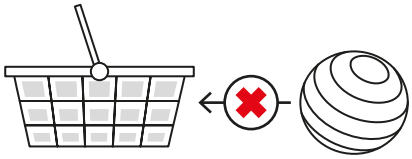
على المستخدم تشخيص التغييرات التي قد تطرأ على طبيعة عمل جهاز الحاسوب الخاص به، والتي قد تكون مؤشرًا لإصابة الجهاز بالبرمجيات الضارة، ومن هذه الحالات:

- وجود بطء في أداء الحاسوب.
- حدوث أعطال فجائية في الجهاز.
- عرض رسائل خطأ متكررة.
- عدم القدرة على إغلاق أو إعادة تشغيل الحاسوب.
- عرض الحاسوب لمجموعة كبيرة من النوافذ المنبثقة.
- عرض الحاسوب لإعلانات غير مناسبة تتداخل مع محتوى الصفحة.
- عدم استجابة الحاسوب لمحاولات إزالة البرامج غير المرغوب بها.
- وجود إعلانات لا نراها عادة في بعض المواقع مثل المواقع الحكومية.
- عرض صفحات ويب لم نقم بزيارتها.
- إرسال رسائل بريد إلكتروني لم نكتبها.
- وجود أشرطة أدوات أو رموز جديدة وغير متوقعة في المتصفح أو على سطح المكتب.
- حدوث تغييرات غير متوقعة في المتصفح، مثل استخدام محرك بحث افتراضي جديد أو عرض علامات تبويب جديدة لم نفتحها.
- حدوث تغيير مفاجئ أو متكرر في الصفحة الرئيسة لمتصفح الإنترنت.
- استنزاف بطارية الحاسوب المحمول بسرعة أكبر مما ينبغي.

التعامل مع البرمجيات الضارة

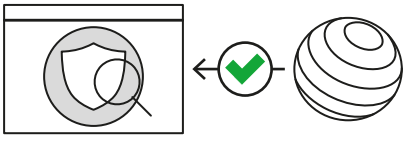
يتعين اتخاذ الخطوات التالية في حالة الاشتباه بوجود برمجيات ضارة على حاسوبنا:

> التوقف عن القيام بالتسوق الإلكتروني واستخدام الخدمات المصرفية على الحاسوب، وعدم القيام بأي أنشطة أخرى عبر الإنترنت تتضمن أسماء المستخدمين أو كلمات المرور أو غيرها من المعلومات الحساسة.

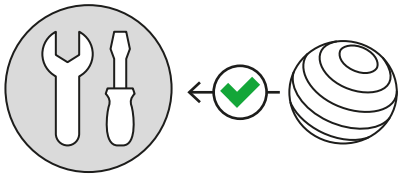


> تحديث برنامج الحماية، ثم القيام بفحص الحاسوب بحثًا عن الفيروسات وبرامج التجسس، مع حذف العناصر المشتبه بها، ثم إعادة تشغيل الحاسوب لتطبيق التغييرات التي قد تمت.

> التحقق من المتصفح لمعرفة ما إذا كان به أدوات لحذف البرامج الضارة، ومن الممكن أيضًا إعادة تعيين المتصفح إلى إعداداته الافتراضية.



> يمكن الاستعانة بالدعم الفني من خلال الاتصال بالشركة المصنعة لجهازك، جهز الرقم التسلسلي قبل الاتصال بالشركة المصنعة للحاسوب، وتأكد من معرفتك للبرامج التي تم تثبيتها ومن قدرتك على تقديم وصف موجز للمشكلة.



هجوم الفدية (الابتزاز المالي) Ransomware

هناك شكل آخر ظهر حديثًا للبرمجيات الضارة وهو برمجية هجوم الفدية، والذي تم تصميمه لقفل جهاز الحاسوب أو منع الوصول إلى ملفاته لابتزاز الضحية بدفع أموال مقابل إلغاء تأمين هذا القفل، وفي الغالب يرى المستخدم على الشاشة نافذة تُعلمه عن هجوم الفدية وطلب الدفع. لا يمكن للمستخدم إغلاق هذه النافذة، وتمنع البرمجيات الخبيثة المستخدم من أداء أية وظائف على حاسوبه الخاص.

وقد يكون هذا النوع من الهجمات خطيرًا للغاية إذا كانت هناك مواد حساسة على الحاسوب أو في حالة كان هذا الحاسوب يُستخدم لتشغيل شركة أو مؤسسة ما. لقد ازدادت هجمات طلب الفدية بشكل مضطرد، حيث يميل الضحايا إلى الاستسلام لهؤلاء المجرمين والدفع لهم من أجل استرجاع أعمالهم أو ملفاتهم والتي قد تكون استغرقت أعوامًا من العمل المتواصل. إن أهم طريقة للوقاية هي وجود برنامج جيد لمكافحة البرمجيات الضارة.

نصيحة ذكية

يحتوي نظام التشغيل Windows 10 على ميزة "استعادة النظام" المُفعلة افتراضيًا، مما يعني إمكانية استعادة الحاسوب إلى النقطة التي سبقت حدوث الإصابة.

قائمة التحقق من أمن أجهزة الحاسوب

- ◯ **التحقق من جهاز التوجيه Router** يجب أن تكون كلمة مرور جهاز التوجيه وكلمات الوصول محفوظة في مكان آمن.

- ◯ **التحقق من الشبكة اللاسلكية Wi-Fi** يجب التحقق من استخدام خيار أمان **WPS2** للشبكة اللاسلكية، كما يجب التحقق من الأجهزة المتصلة حاليًا بحثًا عن أي نشاطات مشبوهة أو غير طبيعية، وفي حالة استخدامك لأي شكل آخر من أشكال أمان جهاز التوجيه فيجب التحقق من كونها لا زالت تعمل نظرًا لأن التحديثات يمكنها إعادة تعيين أجهزة التوجيه.

- ◯ **التحقق من موقع الشبكة اللاسلكية** يجب استخدام تطبيق **Wi-Fi Analyzer** على الهاتف المحمول أو الجهاز اللوحي لقياس قوة الإشارة اللاسلكية من جهاز التوجيه، ويجب وضع جهاز التوجيه بحيث تكون الإشارة قوية داخل كافة أجزاء المنزل وليس على مدى طويل في الشارع أو خارج البيت.

- ◯ **التحقق من تحديثات نظام التشغيل** يجب أن يتم تفعيل جميع تحديثات نظم التشغيل الخاصة بالحواسيب أو الهواتف المحمولة المتصلة بالشبكة المنزلية.

- ◯ **التحقق من تحديثات التطبيقات التلقائي** يجب التحقق من عمل التحديثات على البرامج والتطبيقات المستخدمة بشكل دوري، ويفضل إتاحة التحديث التلقائي للبرامج.

- ◯ **التحقق من قائمة البرامج المثبتة** يجب فحص كل حاسوب متصل بالشبكة لمعرفة قائمة البرامج المثبتة، فإذا كان هناك أي برنامج مشبوه، فيجب إزالته فورًا، ومن المفيد جدًا تسجيل البرامج المثبتة (كلقطة شاشة أو ملاحظة) لمقارنتها مع تكرار كل عملية للفحص.

- ◯ **إعادة تعيين كلمة المرور** يوصى بإعادة تعيين كلمة المرور بشكل دوري، فيجب أن يكون لكل مستخدم القدرة على إعادة تعيين جميع كلمات المرور الخاصة بكل موقع يزوره والتأكد من قوة كلمات المرور، يُمكن استخدام برنامج لإدارة كلمات المرور **(Password Manager)** لهذا الغرض.

- ◯ **التحقق من جدار النار** يجب التأكد من تشغيل جدار النار على كل حاسوب لضمان عدم وجود برامج احتيالية ضمن الاتصالات الواردة والصادرة.

- ◯ **النسخ الاحتياطي للبيانات المهمة** يجب القيام بعمليات النسخ الاحتياطي بانتظام لكل حاسوب أو جهاز مع حفظ النسخة الاحتياطية في مكان آمن (بعيد عن الحرائق).

1

ضع علامة ✓ أمام العبارة الصحيحة وعلامة ✗ أمام العبارة الخطأ.

.1	تساعد حماية معلوماتك الشخصية في التقليل من خطر سرقة الهوية أو انتحال الشخصية.	○
.2	تقتصر المعلومات الشخصية على الاسم الكامل والعنوان ورقم الهاتف وتاريـخ الميلاد.	○
.3	يجب الاهتمام أيضًا بأمن الأجهزة الحاسوبية، وذلك بحمايتها من السرقة أو التلف الذي قد يلحق بها أو بالبيانات الإلكترونية.	○
.4	حدوث تغييرات في طبيعة عمل جهاز الحاسوب ليست مؤشراً لإصابة الجهاز بالبرمجيات الضارة.	○
.5	هجوم الفدية مصمم لمنع الوصول إلى الملفات لابتزاز الضحية بدفع أموال مقابل إزالة القفل عن الملفات.	○

2

اذكر أهم الإجراءات المتبعة للوقاية من البرمجيات الضارة.

_____

_____

_____

_____

_____

3

اشرح أربعة من الإجراءات المتبعة للحفاظ على الأمن الإلكتروني الشخصي.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

4

ارجع لقائمة التحقق من أمن جهاز الحاسوب، واستعن بمعلمك لاختيار ثلاثة عناصر من القائمة، والتحقق من توفرها في جهازك.

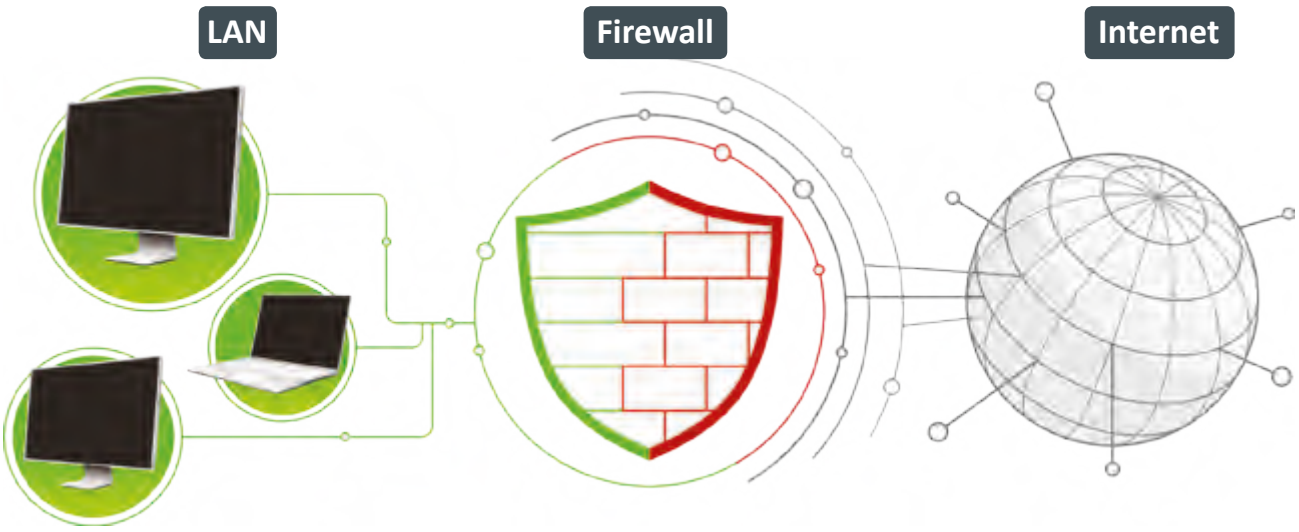
الدرس الثالث

جدار النار والحسابات والأذونات

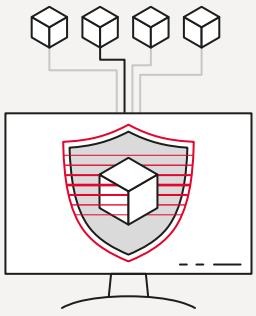
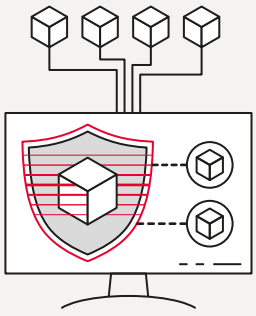
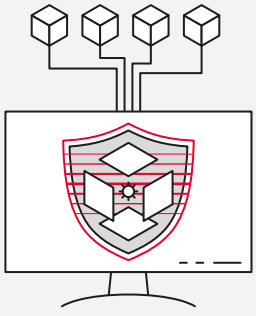
جدار النار Firewall

جدار النار هو برنامج أو جهاز يستخدم لأمان الشبكة ويعتمد على التحكم في حركة نقل البيانات الواردة والصادرة من خلال تحليل حزم البيانات وتحديد ما إذا كان ينبغي السماح لها بالمرور أم لا. يمكن العثور على جدار النار كبرنامج يعمل على حاسوبك، أو قد يكون جهازًا مستقلًا أو مضمناً في أجهزة الشبكات مثل أجهزة التوجيه.

ينشئ جدار النار حاجز أمان يفصل ويحمي جهاز الحاسوب أو الشبكة من الإنترنت، وتتمثل وظيفته الأساسية في حظر الاتصالات المشبوهة.



لنستعرض أجيال جدر النار للحصول على فكرة أفضل عن وظيفتها وقدراتها الحالية.

أجيال جُدر الحماية		
الجيل	الوصف	
الجيل الأول	> يعمل الجيل الأول في طبقة الشبكة **Network Layer**. > يعتمد جدار النار في فحصه للحزم على المعلومات التي يقوم بحملها بروتوكول **TCP/IP** في الحزمة. > يفحص جدار النار كل حزمة على حدة للتأكد من مطابقتها لقواعد الأمان الخاصة بالشبكة مثلًا السماح للحزم من بروتوكول معين بالمرور وحظر بقية الحزم، أو السماح للحزم القادمة من خادم معين.	
الجيل الثاني	> يعمل الجيل الثاني في طبقة الشبكة **Network Layer** أيضًا ويفحص الحزم بناء على معلومات بروتوكول **TCP/IP** في الحزمة. > يفحص الجيل الثاني من جدار النار مجموعة الحزم ويحتفظ بها في ذاكرة وسيطة لحين توفر معلومات كافية لإصدار حكم بشأنها، بحيث يكشف الجدار عن نوع الحزمة إذا كانت بداية اتصال فيتم فحصها، أو جزء من اتصال موجود فيتم تمريرها مباشرة، أو ليست جزءًا من أي اتصال فيتم فحصها كذلك، ويسمى هذا بالتفتيش الدقيق للحزم.	
الجيل الثالث	> يعمل الجيل الثالث في طبقة التطبيقات **Application Layer** ويقوم بفحص البيانات من خلال تصفية البروتوكولات عالية المستوى مثل **FTP** و**DNS** و**HTTP**. > تتجاوز قدرات جدر النار من الجيل الثالث فحص الحزم لتستطيع اكتشاف البرمجيات الضارة وحظرها وإتاحة الدخول للبرمجيات الموثوقة، وكذلك رصد الاستخدام المشبوه لبروتوكولات الشبكة المختلفة وحظره.	

التحقق من جدار النار الخاص بك

يأتي **Microsoft Windows** مزودًا ببرنامج جدار نار، حيث يقوم جدار النار في **Windows** بالعمليات الأساسية مثل حظر الاتصالات الواردة، كما أنه يحتوي على بعض الميزات المتقدمة.

يمكن استخدام جُدر حماية خارجية تتيح لك التحكم بسهولة في تطبيقات حاسوبك التي يمكنها الاتصال بالإنترنت.

لتشغيل جدار النار في Windows:

> اضغط زر **Start**، ❶ اختر **Windows System** (نظام ويندوز). ❷

> اضغط **Control Panel** (لوحة التحكم). ❸

> غير طريقة عرض الإعدادات إلى **Large icons**. ❹

> اضغط **Windows Defender Firewall** (جدار نار ويندوز). ❺

> إذا كان كل شيء يظهر باللون الأخضر فهذا يعني أن جدار الحماية مُفعلًا. ❻

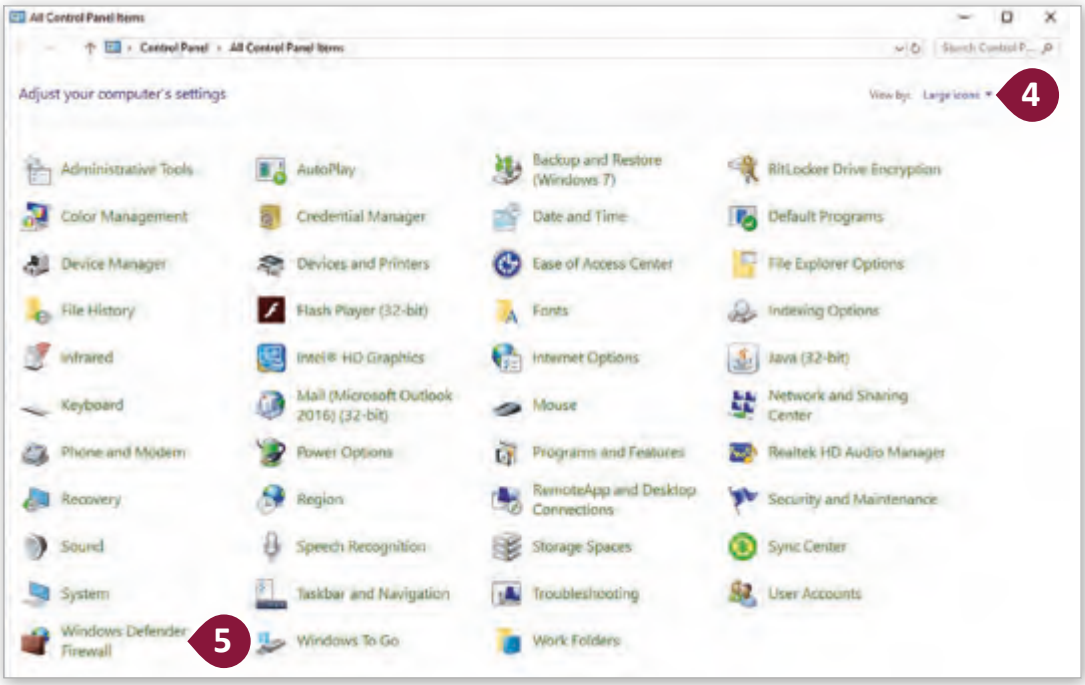
> إذا كان جدار النار لا يعمل، اضغط
Turn Windows Defender Firewall on or off
(تشغيل جدار النار). ❼

> اضغط **Turn on Windows Defender Firewall for all networks**
(تشغيل جدار النار لجميع الشبكات). ❽

> اضغط **OK** (تم). ❾

نصيحة ذكية

لتشغيل أو إيقاف تشغيل جدار النار في Windows، يجب أن تمتلك صلاحيات إدارة النظام في نظام Windows.



يمكنك إيقاف جدار النار في **Windows** الافتراضي في حالة وجود جدار حماية خارجي تعتقد أنه أفضل منه.

السماح للتطبيقات أو منعها

يوفر **Windows** عددًا من ميزات الأمان للحفاظ على جهازك وبياناتك محمية ضد الوصول غير المصرح به ومن البرمجيات الضارة والهجمات الأخرى، وتتضمن تلك الميزات جدار النار الافتراضي.

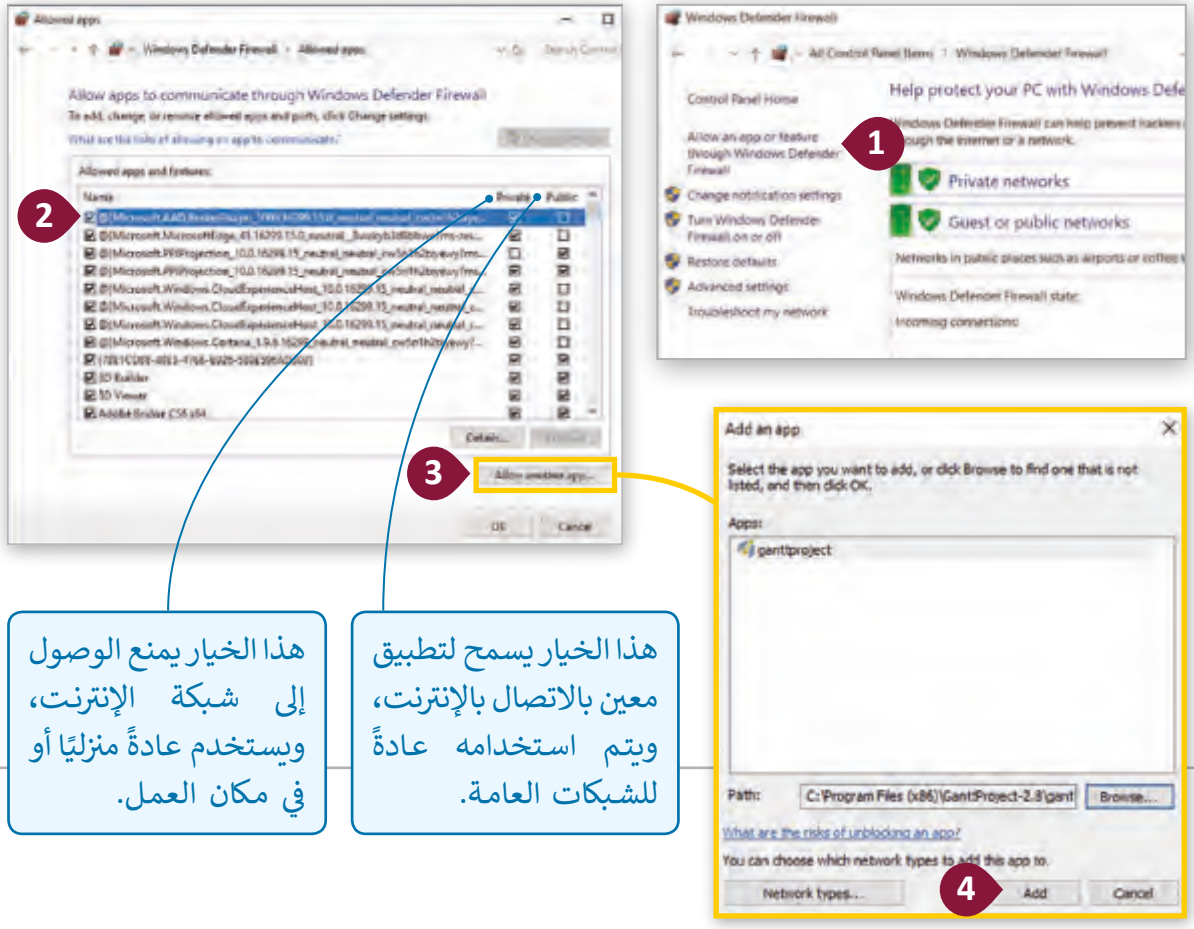
رغم أن هذا الجدار يعمل بشكل جيد عندما يتعلق الأمر بإدارة التطبيقات وتحديد اتصالات الشبكة، إلا أنه قد نحتاج في بعض الأحيان إلى السماح أو منع التطبيقات يدويًا.

للسماح للتطبيقات أو منعها يدويًا:

> من نافذة **Windows Defender Firewall** (جدار النار في ويندوز)، اضغط **Allow an app or feature through Windows Defender Firewall** (السماح لتطبيق أو ميزة من خلال جدار النار في ويندوز). ❶

> ستظهر قائمة بالتطبيقات المثبتة التي تطلب الوصول إلى الإنترنت. اضغط على التطبيق الذي ترغب بإضافته إلى القائمة. ❷

> إذا لم يكن التطبيق مُدرجًا في القائمة، اضغط **Allow another app** (السماح لتطبيق آخر). ❸ حدد البرنامج ثم اضغط **Add** (إضافة). ❹



هذا الخيار يسمح لتطبيق معين بالاتصال بالإنترنت، ويتم استخدامه عادةً للشبكات العامة.

هذا الخيار يمنع الوصول إلى شبكة الإنترنت، ويستخدم عادةً منزليًا أو في مكان العمل.

التهديدات التي لا يحمي منها جدار النار:

جدار النار وحده لا يوفر الحماية الكافية ضد جميع تهديدات الإنترنت، فهو لا يحمي من:

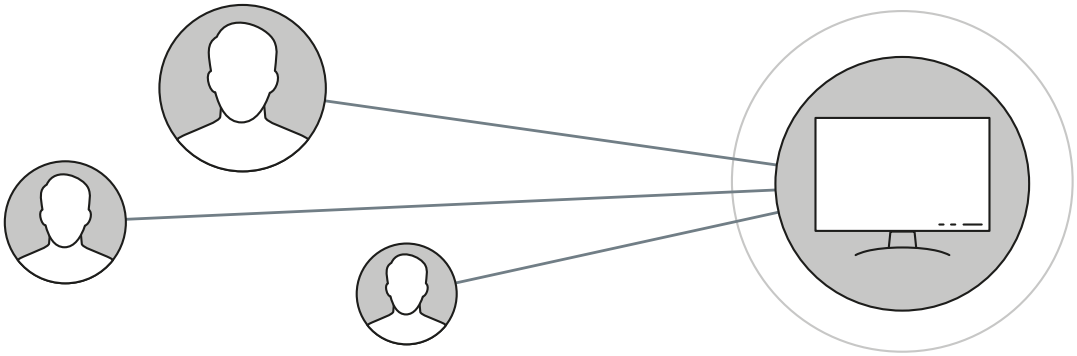
- الاحتيال الإلكتروني.
- الإعلانات المنبثقة.
- البريد المزعج (رسائل البريد الإلكتروني غير المرغوب فيه).

حسابات المستخدم

تطلق تسمية "المستخدم" على كل شخص يستخدم جهاز حاسوب معين. يُمكن إنشاء حسابات متعددة لمستخدمين على نفس الجهاز، حيث يمكن لكل مستخدم تخصيص إعداداته. يمكنك في حساب المستخدم الخاص بك تغيير الإعدادات مثل خلفية سطح المكتب وتنظيم مجلداتك الخاصة وحفظ ملفاتك، كما يمكن أيضًا إدارة سجل تصفح الإنترنت وكلمات المرور من خلال حسابك الخاص.

يتيح **Windows** أربعة أنواع من حسابات المستخدمين:

- حساب المسؤول المدمج (**Built-in administrator account**).
- حساب المستخدم مع امتيازات المسؤول (**User account with administrative privileges**).
- حساب محلي (**Local account**).
- حساب **Microsoft**.



حسابات Microsoft

حساب **Microsoft** هو حساب فردي مجاني يسمح لك بتسجيل الدخول إلى العديد من منتجات وخدمات **Microsoft** ، كما يمكنك باستخدام حساب **Microsoft** تسجيل الدخول إلى حاسوب لم تقم بإعداد حساب مستخدم من قبل عليه.

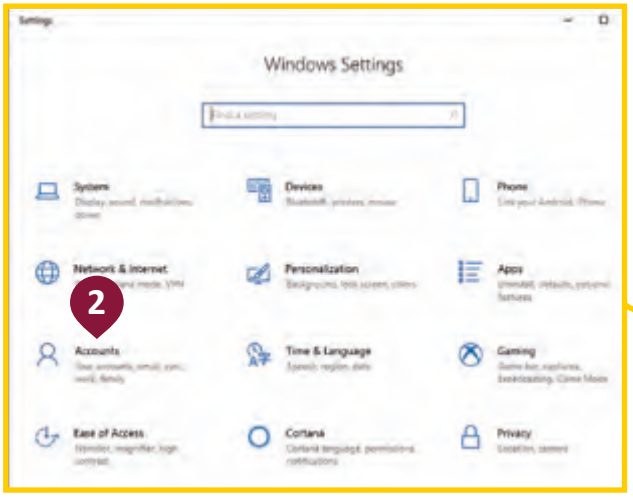
لإضافة حساب Microsoft جديد:

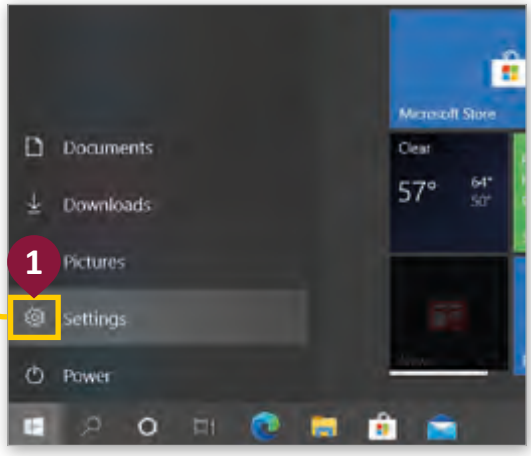
> اضغط فوق زر **Start**، ثم اضغط فوق **Settings** (الإعدادات)، ❶ اضغط **Accounts** (حسابات). ❷

> اضغط فوق **Family & other users** (العائلة والمستخدمين الآخرين) ❸ ومن قسم **Other users** اضغط فوق **Add someone else to this PC** (إضافة شخص آخر إلى هذا الحاسوب). ❹

> أدخل عنوان البريد الإلكتروني للشخص الذي تريد إضافته. ❺ اضغط فوق **Next** (التالي)، ❻ ثم اضغط فوق **Finish** (إنهاء). ❼

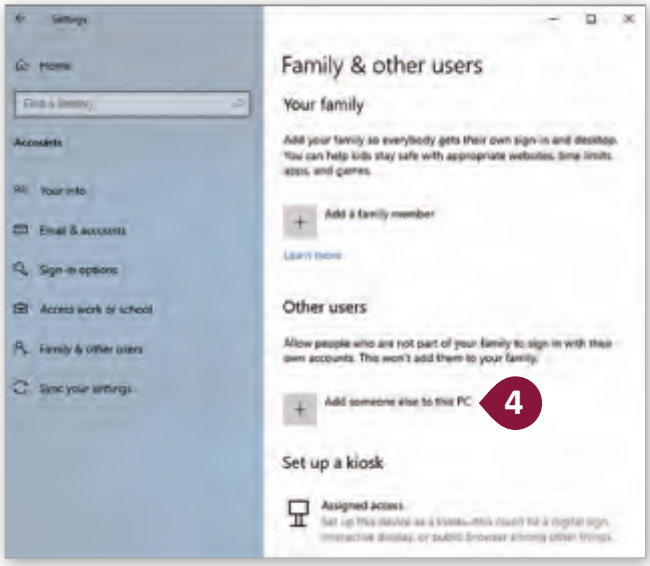
> سيتم إضافة حساب **Microsoft** جديد إلى **Windows**. ❽

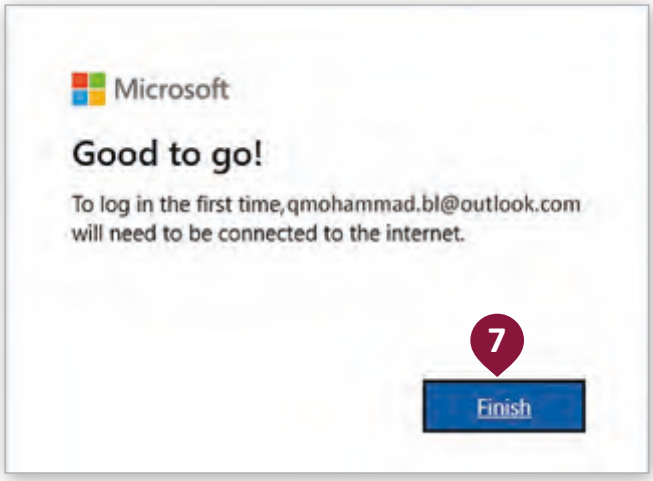


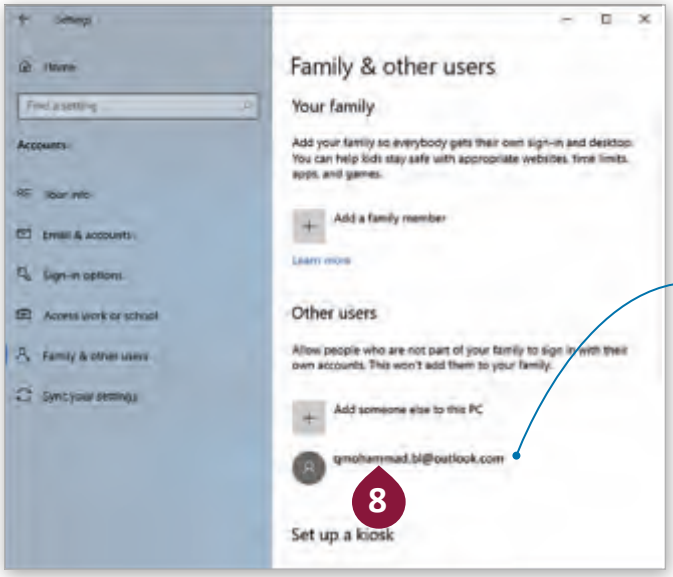


يوفر حساب **Microsoft** إمكانية الوصول إلى خدمات **Microsoft** المتنوعة مثل **Office 365** و**Skype** و**Outlook mail** و**Microsoft Store** و**OneDrive**.

يُمكّنك **Windows** من إعداد حساب **outlook.com** ، و**hotmail.com**، والبريد الإلكتروني **live.com**، أو عنوان البريد الإلكتروني للمؤسسة التي تعمل أو تدرس فيها.







يمكنك من خلال استخدام حساب **Microsoft** مزامنة الإعدادات بين أجهزة حاسوب متعددة، كما يمكّنك من الاحتفاظ بمفضلاتك وسجل التصفح الخاص بك ومعلومات تسجيل الدخول المتزامنة بين حاسوبين أو أكثر.

تسجيل الدخول باستخدام حساب Microsoft

حان الآن وقت تسجيل الدخول باستخدام حساب **Microsoft** الذي أضفته للتو إلى **Windows**، وللقيام بذلك يجب أولاً تسجيل الخروج من حساب المستخدم الخاص بك.

لتسجيل الدخول باستخدام حساب Microsoft:

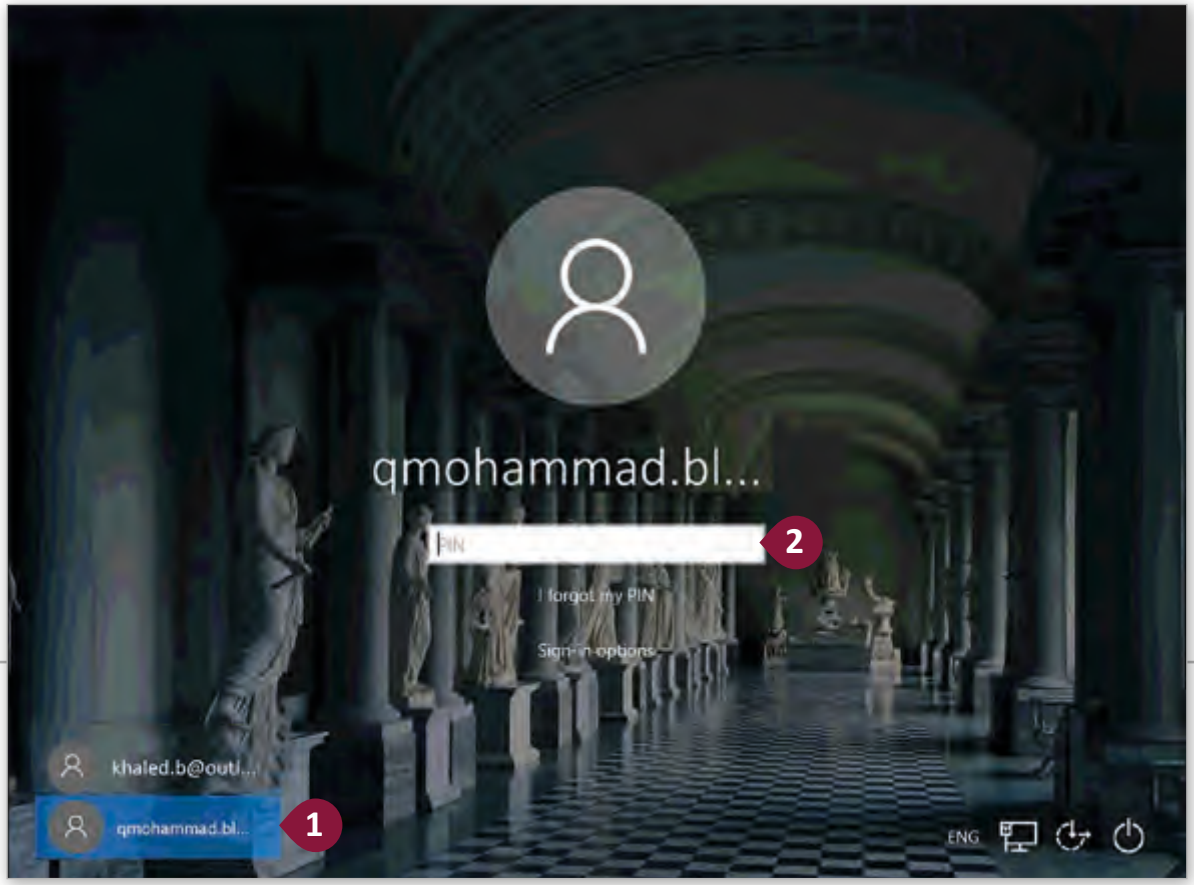
> قم بتسجيل الدخول باستخدام حساب **Microsoft** الذي قمت بإضافته للتو إلى **Windows**. ❶

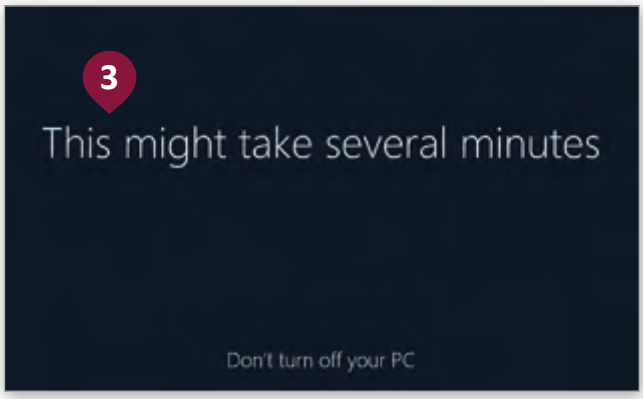
> أدخل كلمة مرور حساب **Microsoft**. ❷

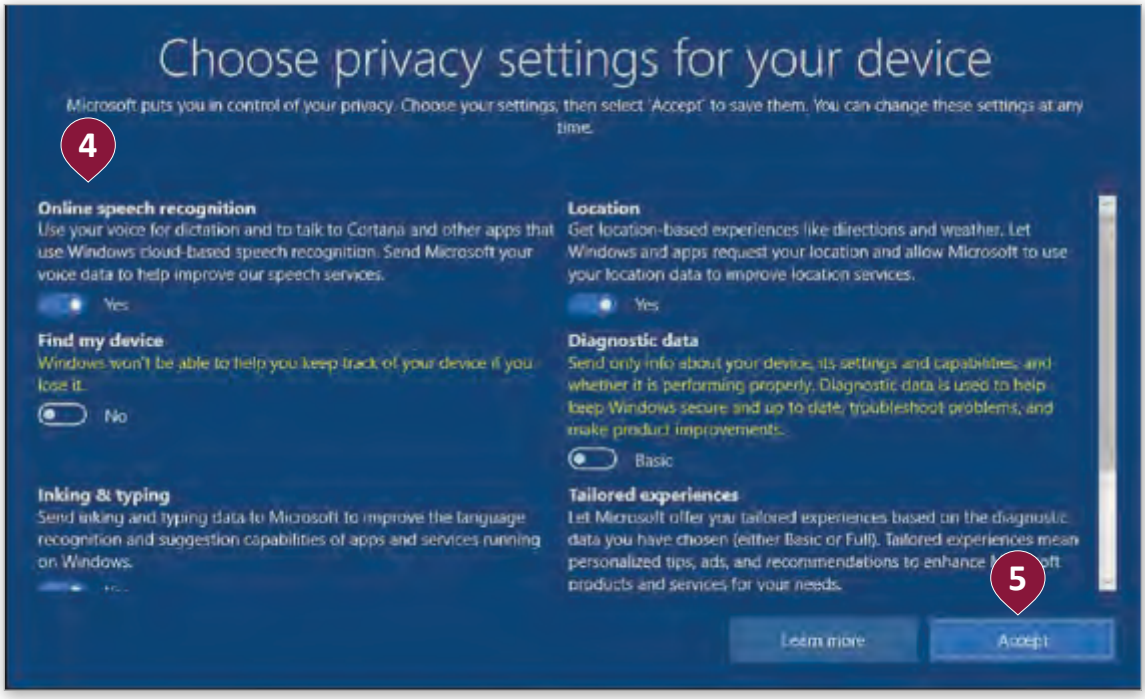
> انتظر لبضع ثوانٍ أو دقائق حتى يقوم **Windows** بإعداد بيئة حساب المستخدم الجديدة. ❸

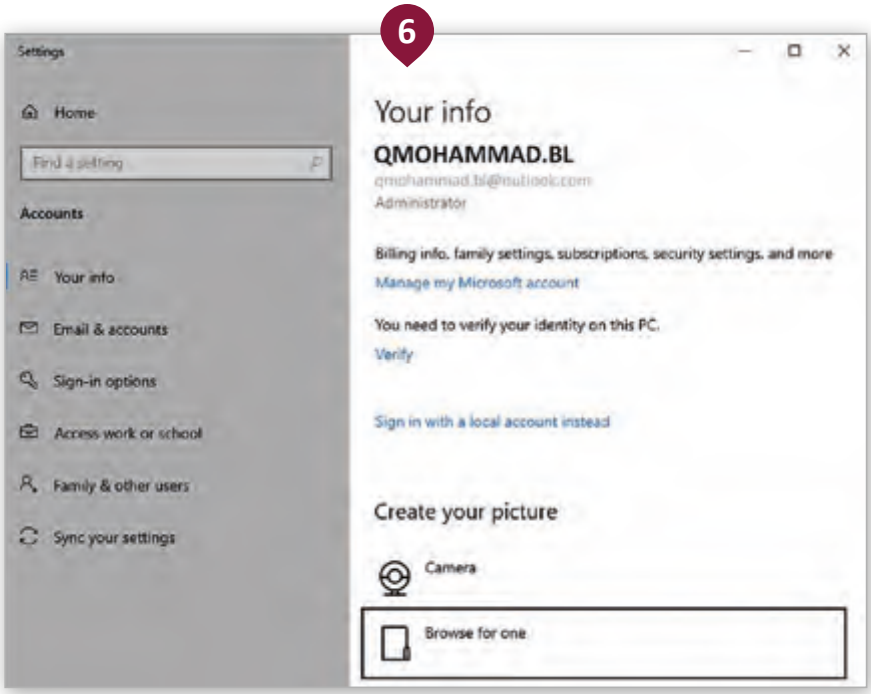
> اختر إعدادات الخصوصية لجهازك، ❹ ثم اضغط فوق **Accept** (قبول). ❺

> سيتم الآن تسجيل دخولك. يمكنك أن ترى أنك قمت بالفعل بتسجيل الدخول باستخدام حساب **Microsoft** الخاص بك من لوحة **Account** (الحسابات) في **Settings** (الإعدادات). ❻




3
This might take several minutes
Don't turn off your PC


Choose privacy settings for your device
Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.
4
Online speech recognition
Use your voice for dictation and to talk to Cortana and other apps that use Windows cloud-based speech recognition. Send Microsoft your voice data to help improve our speech services.
Yes
Find my device
Windows won't be able to help you keep track of your device if you lose it.
No
Inking & typing
Send inking and typing data to Microsoft to improve the language recognition and suggestion capabilities of apps and services running on Windows.
Location
Get location-based experiences like directions and weather. Let Windows and apps request your location and allow Microsoft to use your location data to improve location services.
Yes
Diagnostic data
Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements.
Basic
Tailored experiences
Let Microsoft offer you tailored experiences based on the diagnostic data you have chosen (either Basic or Full). Tailored experiences mean personalized tips, ads, and recommendations to enhance
products and services for your needs.
5
Learn more
Accept


6
Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Sync your settings
Your info
QMOHAMMAD.BL
Administrator
Billing info, family settings, subscriptions, security settings, and more
Manage my Microsoft account
You need to verify your identity on this PC.
Verify
Sign in with a local account instead
Create your picture
Camera
Browse for one

الحسابات المحلية Local Accounts

لا يمكن باستخدام الحسابات المحلية الحفاظ على مزامنة أجهزة الحاسوب أو الوصول إلى خدمات **Microsoft**. يمكنك إنشاء حساب محلي لطفل أو لشخص ليس لديه حساب **Microsoft**، وإذا لزم الأمر يمكنك منح أذونات حساب مسؤول (**Administrator**) لهذا الحساب المحلي.

إنشاء حساب محلي:

> من لوحة **Accounts** (الحسابات) في **Settings** (الإعدادات)، اضغط فوق **Family & other users** (العائلة والمستخدمين الآخرين). ❶

> من قسم **Other users** (المستخدمين الآخرين)، اضغط فوق **Add someone else to this PC** (إضافة شخص آخر إلى هذا الحاسوب).❷

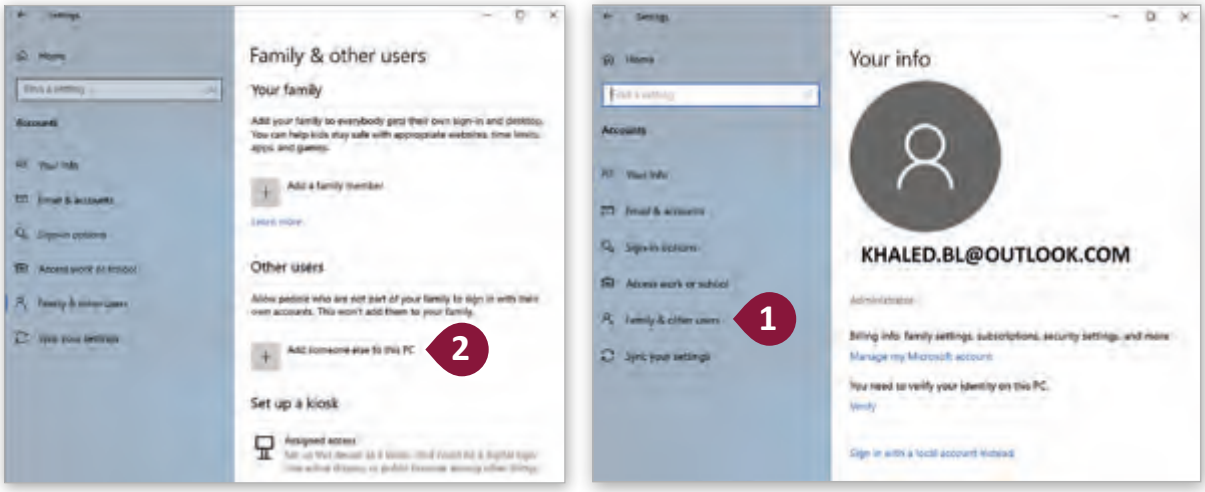
> من قسم **How will this person sign in?** (كيف سيتم تسجيل دخول هذا الشخص)، اضغط **I don't have this person's sign-in information** (ليس لدي معلومات تسجيل الدخول لهذا الشخص). ❸

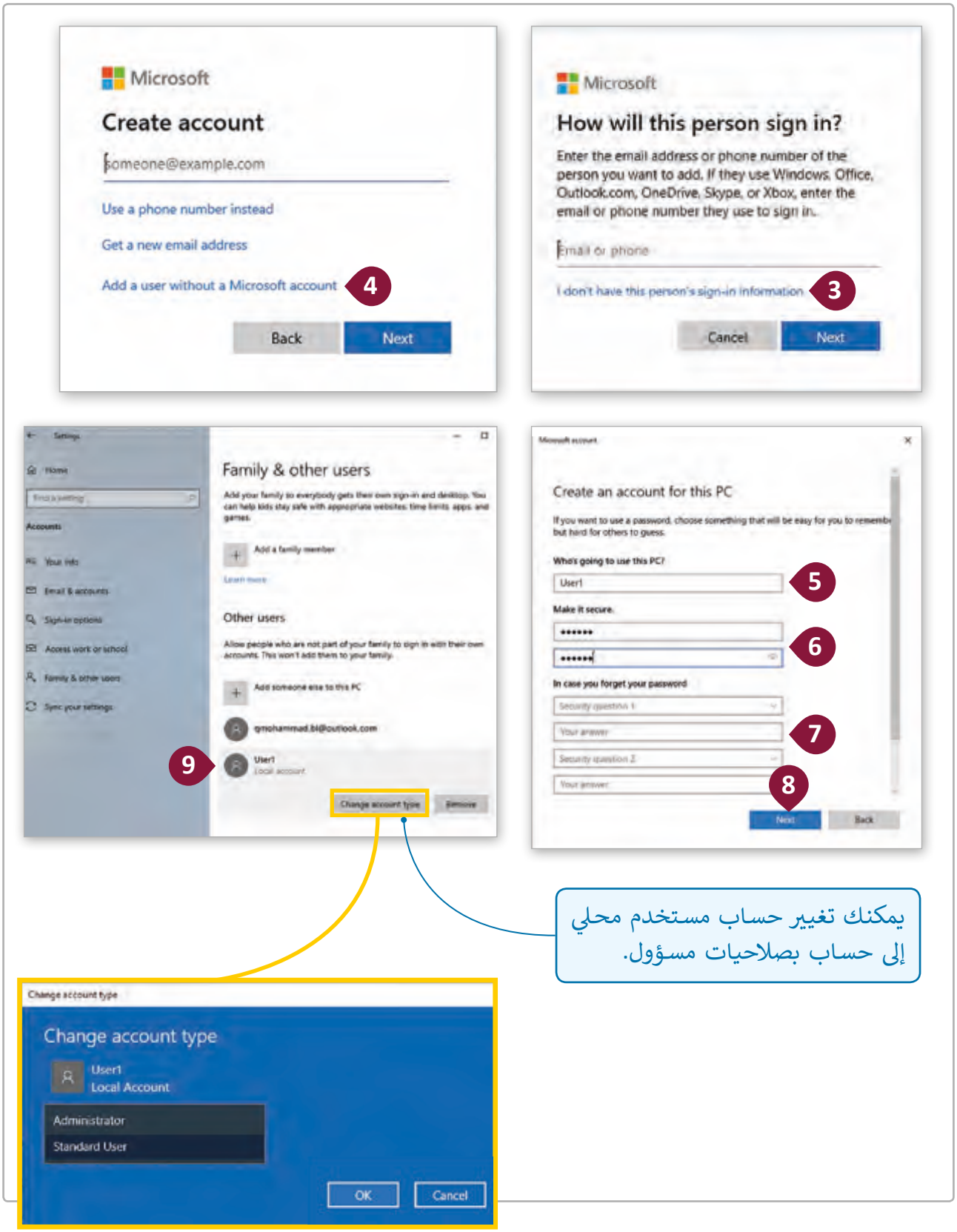
> في مربع حوار حساب **Microsoft**، اضغط فوق **Add a user without a Microsoft account** (أضف مستخدم ليس لديه حساب **Microsoft**). ❹

> أدخل اسم المستخدم ❺ ثم اكتب كلمة المرور مرتين. ❻

> حدد ثلاثة أسئلة أمان مع إجاباتها في حالة نسيان كلمة مرورك. ❼

> اضغط فوق **Next** (التالي) ❽ لكي تنشئ حساب محلي جديد. ❾





نصيحة ذكية

عند استخدام الحسابات المحلية يتم إعداد حساب كل مستخدم للحاسوب بشكل مستقل.

أذونات الملفات والمجلدات File and Folder Permissions

يتمتع كل مستخدم للحاسوب بوجود ملف شخصي وأذونات خاصة به، مما يعني منع الوصول غير المصرح به للملفات والمجلدات، ومع ذلك توجد الحاجة أحيانًا إلى إعداد الأذونات يدويًا على مجموعة من الملفات أو المجلدات لمنع المستخدمين الآخرين من الوصول إلى البيانات.

أنواع الأذونات Permission Types

يتم تطبيق أذونات **NTFS** على كل ملف ومجلد مخزّن على وحدة تخزين مهيأة باستخدام نظام ملفات **NTFS** مثل القرص الصلب لجهاز حاسوب يعمل بنظام **Windows OS**. هناك أنواع مختلفة من أذونات **NTFS** للملفات والمجلدات مثل:

- **Full Control** (التحكم الكامل)
- **Modify** (التعديل)
- **Read & Execute** (القراءة والتنفيذ)
- **List Folder Contents** (عرض محتويات المجلد)
- **Read and Write** (القراءة والكتابة).

نصيحة ذكية

List Folder Contents (عرض محتويات المجلد) هي الإذن الوحيد الحصري الخاص بالمجلدات.

الأذونات	دورها مع الملفات	دورها مع المجلدات
Full Control (التحكم الكامل)	يسمح بالقراءة والكتابة، والتحكم الكامل مثل تغيير أذونات الملف وحذفه ...	يسمح بالقراءة والكتابة والتحكم الكامل مثل تغيير الأذونات والحذف على المجلدات ومحتوياتها من الملفات والمجلدات الفرعية...
Modify (التعديل)	يسمح بالقراءة والكتابة والتعديل، كما يسمح بحذف ا لملف .	يسمح بالقراءة والكتابة على الملفات والمجلدات الفرعية كما يسمح بحذف المجلد.
Read & Execute (القراءة والتنفيذ)	يسمح بعرض الملف وكذلك بتشغيل ملفات البرامج.	يسمح بعرض الملفات والمجلدات الفرعية وتشغيل الملفات التنفيذية (البرامج)، وتطبق نفس الأذونات على الملفات والمجلدات بداخلها.
List Folder Contents (عرض محتويات المجلد)	لا يوجد.	يسمح فقط بعرض الملفات والمجلدات الفرعية وتشغيل الملفات البرمجية، ويتم تطبيق نفس الأذونات على المجلدات الفرعية فقط.
Read (القراءة)	يسمح بعرض الملف أو الوصول إلى محتوياته.	يسمح بعرض الملفات والمجلدات الفرعية.
Write (الكتابة)	يسمح بالكتابة على الملف.	يسمح بإضافة الملفات والمجلدات الفرعية.

تعديل الأذونات

الآن حان الوقت لتعديل بعض الأذونات والتحقق من النتائج. لنستعرض على سبيل المثال كيفية حظر الوصول إلى مجلد خاص بمستخدم معين أو مجموعة معينة.

لتعديل الأذونات الخاصة بمستخدم محدد:

> اضغط بزر الفأرة الأيمن ملف أو مجلد، ثم اضغط **Properties** (الخصائص) ❶ ثم اضغط علامة التبويب **Security** (الأمان). ❷

> لتحرير أذونات مستخدم معين، اضغط هذا المستخدم ❸ ثم اضغط زر **Edit** (تحرير). ❹

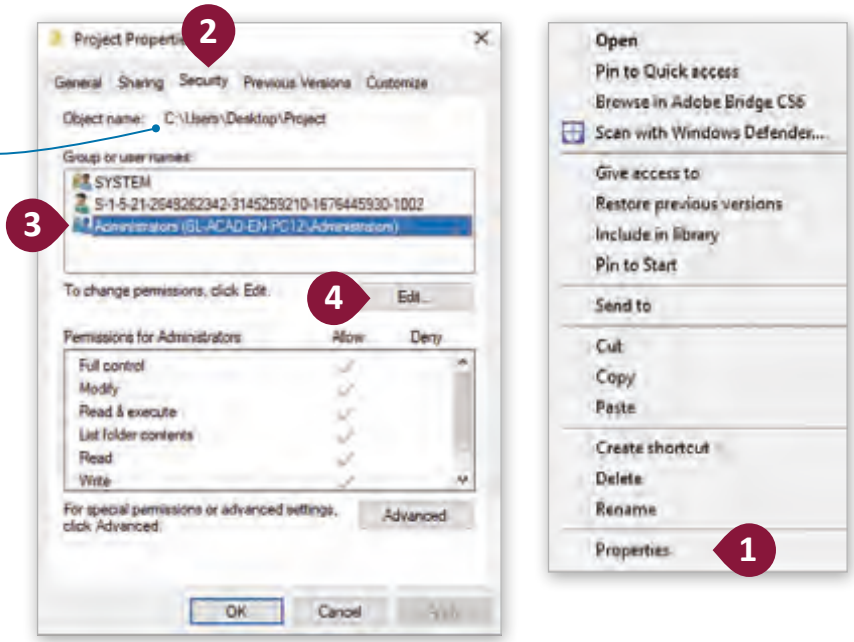
> اضغط زر **Add** (إضافة)، ❺ وبعد إضافته يمكنك تحديد خيار زر **Deny** (المنع) بجانب **Full Control** (التحكم الكامل).

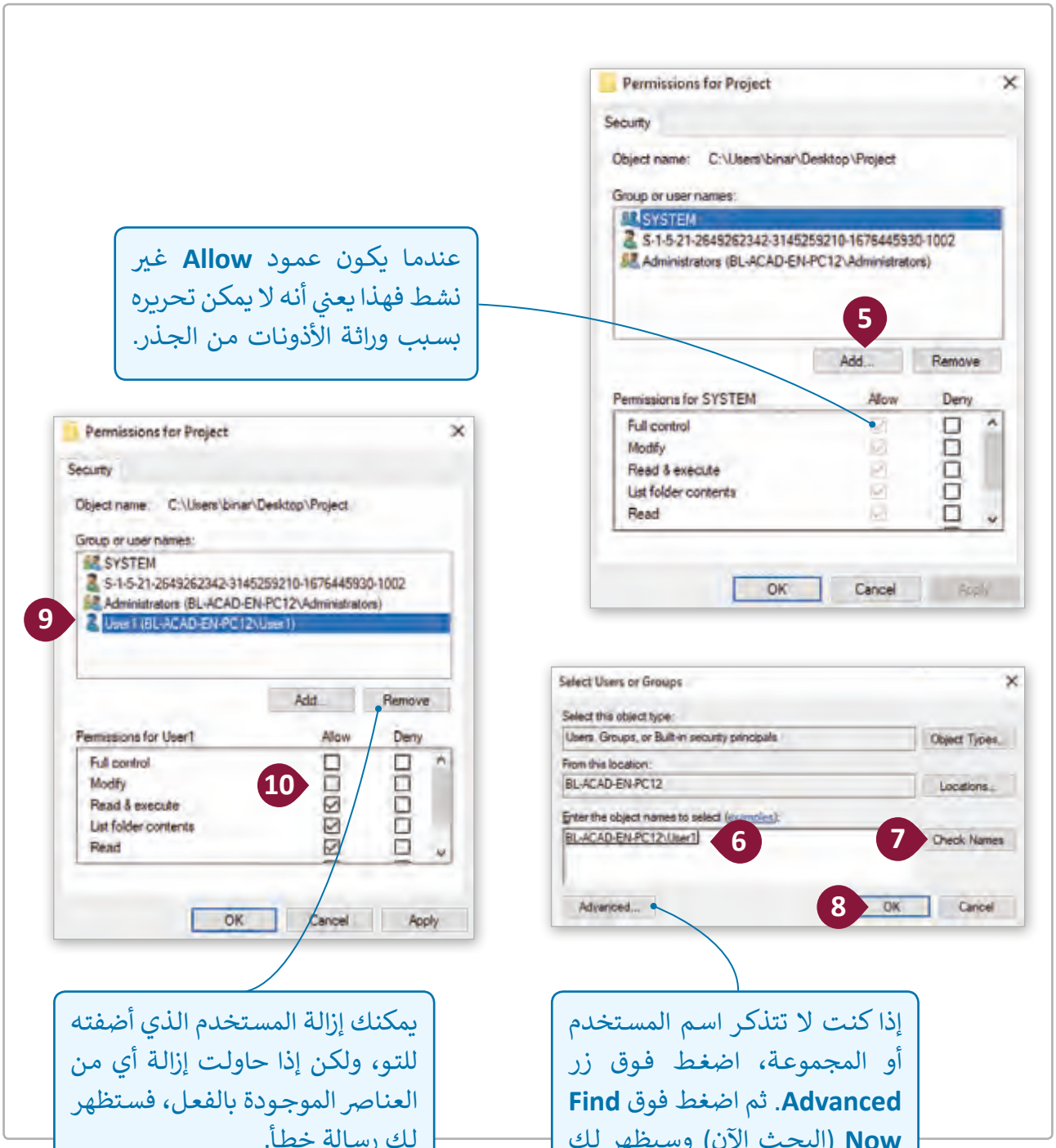
> من نافذة **Select Users or Groups** (تحديد المستخدمين أو المجموعات)، اكتب اسم المستخدم، ❻ اضغط **Check Names** (التحقق من الأسماء) للتأكد من صحتها. ❼

> اضغط **OK** (تم). ❽ سيتم إضافة المستخدم أو المجموعة إلى قائمة **Access Control** (التحكم في الوصول). ❾

> الآن يمكنك اختيار عمود **Allow** (السماح) أو **Deny** (المنع). ❿

يتم توريث الأذونات أيضًا في نظام **Windows**، حيث يحصل كل ملف أو مجلد على أذونات من المجلد الأصل/ ويستمر هذا التسلسل الهرمي وصولًا إلى جذر القرص الصلب.





نصيحة ذكية

كي تتمكن من تحرير أي أذونات، يجب أن تتوافر لديك ملكية الملف أو المجلد، فإذا كان المالك هو حساب مستخدم آخر أو حساب نظام مثل النظام المحلي، فلن تتمكن من تعديل الأذونات.

1

عرف جدار النار، وقارن بين أجياله الثلاثة من حيث طبقة الشبكة التي يعمل عليها والبروتوكولات التي يستخدمها وآلية العمل.

_____

_____

_____

_____

_____

_____

2

صف الإجراءات التي يجب اتباعها للتحقق من جدار النار الخاص بـ **Windows** على جهاز الحاسوب الخاص بنا والسماح بتطبيقات معينة أو حظرها ، استعن بحاسوبك للتحقق من صحة الخطوات.

_____

_____

_____

_____

_____

3

اذكر أربعة من الأذونات المستخدمة على وحدات التخزين المهيأة بنظام **NTFS**، وحدد دورها مع كل من الملفات والمجلدات.

الدرس الرابع

البصمة الرقمية وأمن الإنترنت

إن كل عملٍ أو تصفحٍ نقوم به عبر الإنترنت يترك أثرًا يسمى "البصمة الرقمية"، والتي قد يتمكن الآخرون من رؤيتها، وذلك ينطبق أيضًا على تاريخ التصفح والمواقع التي نقوم بزيارتها، يهدف ذلك إلى توفير تجربة تصفح أسرع وأكثر كفاءة للمستخدم أو لاستهدافه من قبل المعلنين عبر الإعلانات المخصصة التي تظهر عبر الإنترنت.

البصمة الرقمية Digital Footprint

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.

البصمات الرقمية النشطة Active Digital Footprints

تنشأ البصمات الرقمية النشطة من البيانات التي نتركها بمجرد تنفيذنا للنشاطات المختلفة عبر شبكة الإنترنت.

أمثلة على البصمات الرقمية النشطة:

- المنشورات على مواقع **Facebook** أو **Instagram** أو**Twitter** وأي منصة من منصات التواصل الاجتماعي.
- الموافقة على تثبيت ملفات تعريف الارتباط **Cookies** على أجهزتنا عند طلب المتصفح لذلك.
- النماذج التي تُعبأ عبر الإنترنت، مثل نموذج الاشتراك لتلقي رسائل البريد الإلكتروني أو الرسائل النصية.

البصمات الرقمية المجهولة Passive Digital Footprints

البصمات الرقمية المجهولة هي تلك التي نتركها وراءنا دون قصد أو في بعض الحالات دون أن نعرف ذلك.

أمثلة على البصمات الرقمية المجهولة:

- التطبيقات والمواقع التي تستخدم تحديد الموقع الجغرافي لتحديد موقع المستخدم.
- مواقع الويب التي تثبت ملفات تعريف الارتباط في أجهزتنا دون إخطار المستخدم.
- وسائل التواصل الاجتماعي والأخبار والقنوات والمعلنين الذين يستخدمون إعجابات المستخدمين ومشاركاتهم وتعليقاتهم للتعرف عليهم وتقديم الإعلانات المخصصة بناءً على اهتماماتهم.

البيانات المسجلة أثناء استخدام الإنترنت

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.
- هوية الحاسوب الذي يقوم بالاتصال.
- مُعرف 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).

تُسمى هذه البيانات بسجلات الخادم (**Server Logs**) وهي الأساس لتحليلات الويب، ومن الجدير بالذكر أنه لا يمكن رؤيتها إلا من قبل مالكي الموقع. إن نفس الخوادم التي تقدم لنا مواقع الويب تتبع سجلات تصفحنا بشكلٍ صامت (دون علمنا). وتقوم بكل بساطة بتعيين رقم خاص بجهازنا ثم تتبع كل ما نتصفحه بكل سهولة.

آثار التعقب الرقمية Digital Traces

آثار التعقب الرقمية هي مثل الآثار الطبيعية وتتراكم لإنشاء بصمتنا الرقمية. تتضمن "البصمة الرقمية" الخاصة بنا جميع آثار نشاطنا عبر الإنترنت بما في ذلك تعليقاتنا على المقالات الإخبارية والمنشورات على وسائل التواصل الاجتماعي وسجلات عمليات الشراء عبر الإنترنت.

يوجد نوعان من آثار التعقب الرقمية:

- الآثار المقصودة والمرئية مثل رسائل البريد الإلكتروني أو النصوص أو مشاركات المدونات أو مشاركات **Twitter** أو الصور الفوتوغرافية أو التعليقات على مقاطع فيديو **YouTube** أو الإعجابات على **Facebook**.
- الآثار غير المقصودة وغير المرئية مثل سجلات زيارات المواقع وعمليات البحث والسجلات المتعلقة بتحركات المستخدم على الشبكة وعمليات التواصل التي يجريها مع الآخرين.

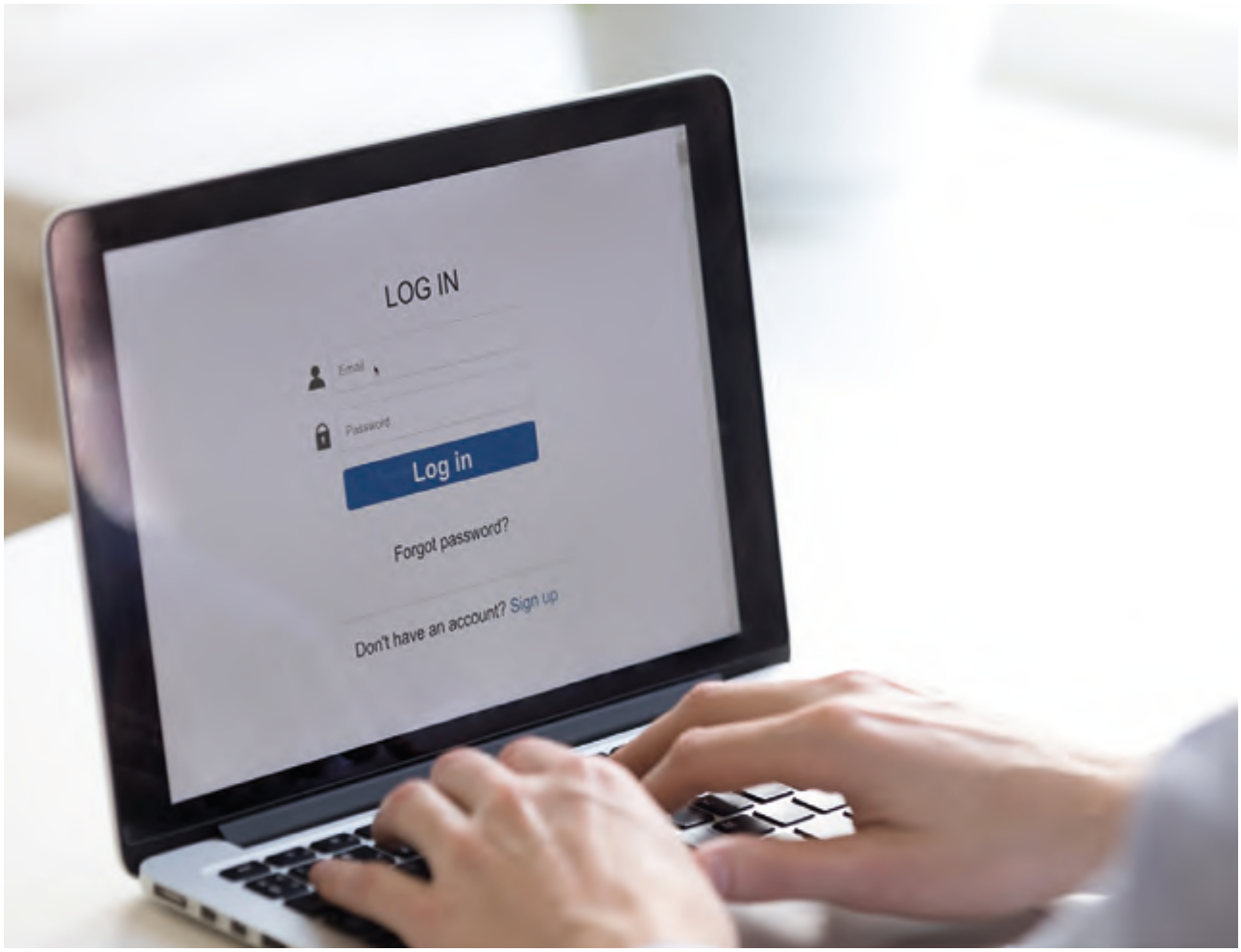
يمكن الحصول على صورة واضحة حول تفاصيل حياتنا - بما في ذلك التفاصيل التي نفترض أنها خاصة – من خلال تعقب الآثار المرئية وغير المرئية معًا.

مصادر المعلومات الشخصية وتبعات تداولها

يجب أن نكون على دراية بما تملكه شركات التكنولوجيا من معلوماتنا الخاصة ومن أين تستقيها، وكيف تستخدم هذه المعلومات.

مصادر البيانات والمعلومات الشخصية:

- قد تأتي من المستخدم مباشرة عند قيامه بإدخال الاسم وعنوان البريد الإلكتروني ورقم الهاتف الخاص به على مواقع التسوق أو مواقع التواصل الاجتماعي مثل **Facebook**.
- المعرفات الفريدة الخاصة بجهاز الحاسوب مثل التطبيقات ونظام تحديد المواقع العالمي **(GPS)** وبيانات المستشعرات الخاصة بأجهزتنا وكذلك المعلومات الملتقطة من قبل الأجهزة المحيطة بنا مثل نقاط وصول **Wi-Fi**.
- مصادر متاحة للجمهور مثل الصحف المحلية وشركاء التسويق من جهات خارجية والمعلنين، وغيرها ....



قد يترتب على تداول البيانات الشخصية للمستخدمين ما يلي:

- مرور البيانات عبر شبكات قابلة للاختراق.
- تخزين تلك البيانات في قواعد بيانات قد يتم سرقتها أو بيعها.
- حفظ تلك البيانات على الأقراص الصلبة والهواتف الذكية وأجهزة الحاسوب حيث يتمكن بعض الأفراد من الوصول إليها.
- إتاحة البيانات للباحثين الأكاديميين وللسلطات والمحاكم وكذلك للعديد من الشركات التي تحاول بيع منتجاتها لنا.

في الاقتصاد المبني على البيانات، يخضع سلوكنا: أولًا للتعقب والتحليل والفهرسة، ثم للتنبؤ به وتعديله.

وجود المعلومات المشاركة بشكل دائم عبر الإنترنت

علينا أن ندرك أن جميع المعلومات المتداولة من خلال الانترنت تسجل بشكل دائم.

عند استخدام الحاسوب أو أي تقنية معلومات أخرى، يتم تخزين سجل رقمي مفصل للبيانات التي تتم معالجتها أو نقلها على كل من:

- القرص الصلب لجهاز المستخدم.
- خادم مزود خدمة الإنترنت إذا كان الاستخدام عبر الإنترنت.
- من المحتمل أن يحتفظ بها في قواعد بيانات حكومية أو خاصة.

تقوم شبكة الإنترنت بفهرسة صفحات الويب ومحتوى الويب أسبوعيًا كحد أدنى، وتتوفر حاليا على الإنترنت بيانات محفوظة منذ منتصف التسعينات وبمجرد نشرنا للمعلومات، علينا أن ندرك أن أية معلومة نقوم بنشرها قد تبقى على شبكة الإنترنت إلى الأبد. وعلى الرغم من أن خبراء الحاسوب قد يتمكنون من استرداد المحتوى عبر الإنترنت وتدميره، إلا أنه لا توجد ضمانات بشأن ذلك. وعليه فإنه يجب أن نضع في الاعتبار أن نشر المعلومات الشخصية بصورة مفرطة على الإنترنت يعني زيادة الفرص لبعض الأفراد أن يستخدموا تلك المعلومات بطريقة غير مناسبة.

هل تعلم أن رسائل البريد الإلكتروني المحذوفة من قِبَلْ كل من المرسل والمستقبل قد تبقى منها نسخ احتياطية في مكان ما؟

كيف تتصفح الشبكات الاجتماعية بشكل آمن؟

كن حذرًا من مشاركة الكثير من المعلومات.
لا تشارك أية معلومات خاصة مثل الرقم الشخصي أو تاريخ ومكان الميلاد، حيث أن ذلك قد يعرضك لأخطار سرقة الهوية والاحتيال.

الضبط الصحيح لإعدادات الخصوصية.
تحتوي جميع مواقع الشبكات الاجتماعية تقريبًا على إعدادات خصوصية محددة مسبقًا أو افتراضية تُمكننا من حجب بعض المعلومات عن الغرباء وغير الأصدقاء، كما وتحُدُّ هذه الإعدادات أيضًا من المعلومات المتوفرة في نتائج البحث. يُمكننا دومًا تعديل إعدادات الخصوصية لمزيد من الحماية.

تحديد التفاصيل التي يتم مشاركتها حول الوظيفة ومكان العمل.
يمكن أن تكشف المعلومات المتعلقة بالعمل الكثير عن حياتنا الشخصية ويمكن أن تمنح لمجرمي الإنترنت مثل المتسللين الكثير من المعلومات الشخصية التي تساعدهم على اختراق حسابنا أو سرقة هويتنا.

تحقق من شخصية الأشخاص الذين تتواصل معهم.
عليك التحقق من صحة حساب من يقوم بإضافتك كصديق من خلال وسائل التواصل الاجتماعي.

كن حذرا عند القيام بوضع التعليقات وخذ حذرك من انتحال الهوية.
يمكن لأي شخص يشتبه بقيام أحدهم بانتحال شخصيته عبر الإنترنت أن يقوم بالمطالبة بإزالة المنتحل. يمكن الملاحظة أن مواقع الشبكات الاجتماعية باتت تتطلب القيام بالمصادقة لتسجيل الدخول لإضافة المشاركات والتعليقات وغيرها، ...

انتبه من مشاركة تفاصيل حياتك الشخصية.
تشجعنا بعض مواقع الويب على مشاركة الأنشطة التي نقوم بها في جوانب حياتنا المختلفة، ولكن يجب أن ننتبه من عدم الكشف عن معلومات تنبه المجرمين إلى أماكن وجودنا أو أفعالنا الأخرى.

تحقق من حسابك الخاص.
من الحكمة أن يقوم الشخص بالقيام بالبحث عن ملف التعريف الخاص به والتعرف على المعلومات المتوفرة عنه على الإنترنت، ويتيح ذلك للشخص معرفة ما يُمكن للآخرين مشاهدته وتنبيهه إلى وجود معلومات غير مرغوبة أو انتحال للشخصية من خلال حسابات مزورة.

معرفة حدود مكان العمل أو سياسات الاستخدام المقبولة.

من المهم مراجعة السياسات المعمول بها لدى المؤسسة التي تعمل بها، فقد تؤثر هذه السياسات على ما يمكننا مشاركته من معلومات أو صور، وهذا الأمر لا يتم فقط لحماية سمعة الموظفين ولكن أيضًا لمنع فقدان البيانات الخاصة بالعمل أو الملكية الفكرية.

التحكم في المعلومات التي يتم مشاركتها مع مصادر خارجية.

عندما ننضم إلى موقع للتواصل الاجتماعي، يجب أن نفهم كيف يستخدم هذا الموقع المعلومات الخاصة، لذلك يجب قراءة سياسة الخصوصية لمنصات الشبكات الاجتماعية التي تشرح بدقة كيفية استخدام المعلومات الخاصة.

كما يجب إعادة التحقق من شروط الخصوصية بشكل دوري حيث قد تتغير هذه السياسات بما يتيح للشركات بيع معلومات العملاء لآخرين.

كن حذرا من الصداقات الزائدة.

حين تكون عضوًا في مجموعة شبكات اجتماعية، قد يسعدك أن تكتسب "أصدقاء" أو متابعين جدد، ولكن عليك أن تختار الأشخاص الجديرين بالثقة فقط عند قبول طلبات الصداقة الواردة.

ما يتم مشاركته عبر الإنترنت يبقى على الإنترنت.

عند مشاركة المعلومات عبر الإنترنت، من المهم أن تدرك أن ما تكتبه أو تنشره قد يبقى بشكل دائم، وقد تؤثر مثل هذه المشاركات على فرص العمل المستقبلية، وقد تتركك عرضة للجرائم الإلكترونية.

تعرف على كيفية منع المتنمرين.

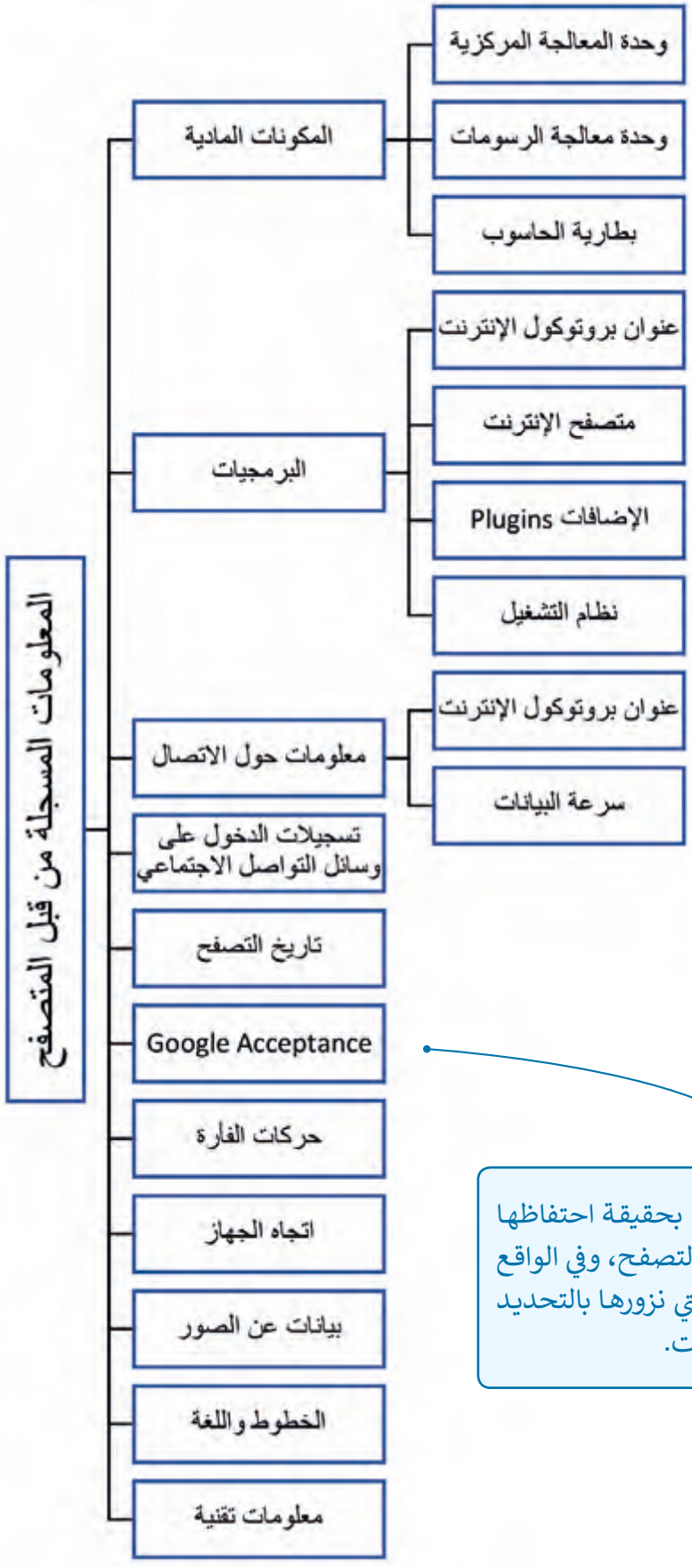
عند الانضمام إلى شبكة اجتماعية، يجب أن نتعرف على كيفية حظر الأعضاء عند الحاجة، حيث يؤدي حظر الشخص إلى ايقاف قدرته على التفاعل مع من قام بحظره.

قم باستخدام كلمات المرور القوية.

من المهم اختيار كلمة مرور تتكون من ثمانية رموز على الأقل وتدمج ما بين الأحرف والأرقام، كما يجب تغييرها بشكل دوري، حيث أن إنشاء كلمات مرورٍ قوية يمنع المتسللين من الوصول إلى حساباتنا واستخدامها لنشر الرسائل غير المرغوب فيها أو استغلالها للقيام بالهجمات الضارة.

مجموعة البيانات التي يجمعها المتصفح عبر الإنترنت

عنوان بروتوكول الإنترنت متاح دائمًا لأي شخص عن طريق التطبيقات الخاصة بمشاركة الملفات، تطبيقات المراسلة، وحتى الألعاب.



اعترفت شركة **Google** في عام 2018 بحقيقة احتفاظها للسجلات التي يتم حذفها من سجل التصفح، وفي الواقع فإنهم لا يحتفظون بصفحة الويب التي نزورها بالتحديد بل يقومون بتتبع فئات هذه الصفحات.

التعامل مع البيانات التي يخزنها المتصفح

يقوم المتصفح بتخزين البيانات التالي ذكرها، ومن المهم أن نقوم بحذف هذه الملفات بشكل دوري ليس فقط لحماية خصوصيتنا والحفاظ على مستوى الأمان، وإنما أيضًا لنتفادى مشاكل بطء العمل في المتصفح وجهاز الحاسوب بشكل عام.

ملفات تعريف الارتباط Cookies

عند استخدامنا لمتصفح الويب، يتم حفظ بعض المعلومات من مواقع الويب في ذاكرة التخزين وملفات تعريف الارتباط.

توفر ملفات تعريف الارتباط طريقة لموقع الويب للتعرف علينا ومتابعة تفضيلاتنا، فهي ملفات نصية صغيرة تم إنشاؤها بواسطة موقع ويب يتم تخزينها في حاسوبنا إما مؤقتًا لتلك الجلسة فقط أو بشكل دائم على القرص الصلب (ملف تعريف الارتباط الدائم).

من المهم جدًا حذف ملفات تعريف الارتباط **Cookies** عند استخدامنا لأجهزة الحاسوب العامة، كما يستحسن حذفها بشكل دوري من أجهزتنا الخاصة، يستثنى من ذلك في حالة اصطحاب جهاز الحاسوب أثناء السفر، حيث تساعد الملفات في هذه الحالة على مصادقة عمليات تسجيل الدخول إلى خدمات البريد الإلكتروني وغيرها حتى عندما يرصد الجهاز تغيير الموقع إلى بلد آخر.

تاريخ التصفح Browsing history

يتألف سجل التصفح من سجل لصفحات الويب التي قمنا بزيارتها في جلسات التصفح السابقة، وعادةً ما يتضمن اسم الصفحة وموقع الويب بالإضافة إلى عنوان **URL** المقابل لها، ولكل متصفح ويب واجهته الفريدة التي تسمح لنا بإدارة أو حذف محفوظات التصفح من محرك الأقراص الثابتة لدينا.

كلمات المرور المحفوظة

عند زيارتنا لموقع ويب يتطلب تسجيل الدخول، فإن متصفح الويب يسأل عما إذا كنت تريد تذكر اسم المستخدم وكلمة المرور، فإذا اخترت نعم فإنه في المرة القادمة التي نزور فيها الموقع يقوم متصفح الويب بتعبئة معلومات الحساب الخاصة بنا.

يتم تشغيل خاصة حفظ كلمة المرور افتراضيًا، ولكن يمكننا إيقاف تشغيل هذه الخاصية أو مسح كلمات المرور المحفوظة.

لحذف ملفات تعريف الارتباط وتاريخ التصفح وكلمات المرور المحفوظة:

> افتح برنامج **Microsoft Edge** واضغط **Settings and more** (الإعدادات والمزيد). ❶

> اضغط **Settings** (الإعدادات). ❷

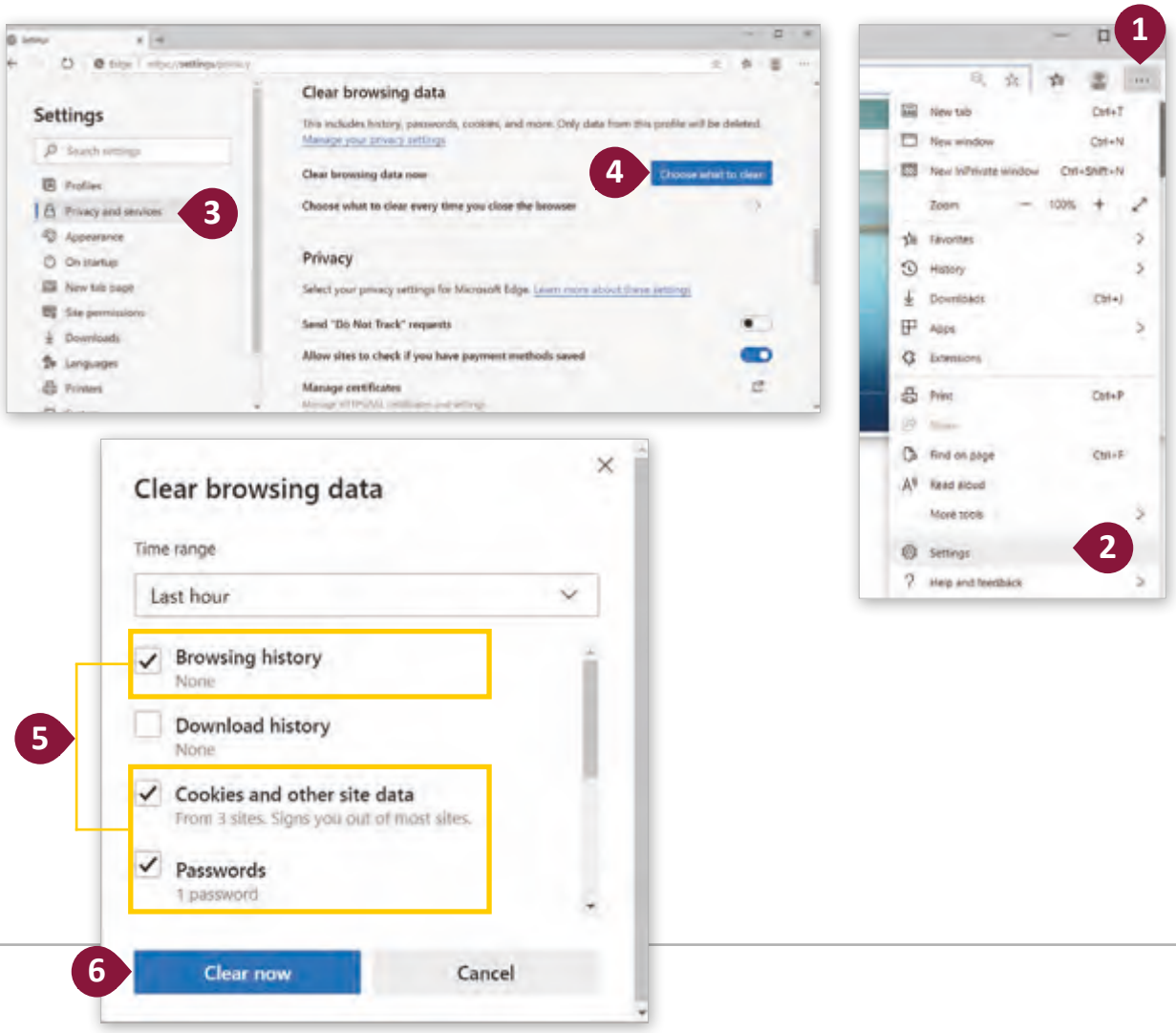
> اضغط **Privacy and services** (الخصوصية والأمان). ❸

> تحت **Clear Browsing data** (مسح بيانات الاستعراض) اضغط **Choose what to clear** (اختر ما تريد مسحه). ❹

> اختر ما تريد مسحه الآن. ❺

> اضغط **Clear now** (المسح الآن). ❻

> لقد تم حذف ما قمت بتحديده.



تعطيل النوافذ المنبثقة pop-up في المتصفح

النوافذ المنبثقة هي نوافذ صغيرة "تنبثق" أعلى صفحات الويب في متصفح الويب.

يتم استخدام هذه النوافذ من المعلنين كوسيلة لجذب الانتباه، ولكنها سرعان ما أصبحت مصدر إزعاج للمستخدمين، مما جعل مطوري البرمجيات والمتصفحات يطورون برمجيات حظر النوافذ المنبثقة، ونتيجة لذلك تم تقييد بعض الاستخدامات الجيدة للنوافذ المنبثقة - على سبيل المثال عرض معلومات مفيدة أو عرض مقاطع الفيديو.

تحاول الشركات استخدام النوافذ المنبثقة للحصول على تفاصيل الاتصال بالمستخدم، على سبيل المثال عنوان البريد الإلكتروني، ولذا أصبحت صناديق بريدنا الإلكتروني تزدحم برسائل البريد الإلكتروني الإعلانية.

يمكن لبعض النوافذ المنبثقة تثبيت ما يُسمى **Trojan horse** (حصان طروادة) الذي يقوم بتحميل تطبيقات ضارة أخرى على النظام الخاص بنا أو تثبيت برنامج لتسجيل ضغطات المفاتيح مما يمنحه القدرة للوصول لأي بيانات سرية مالية أو ضريبية أو حتى كلمات المرور لحساباتنا المصرفية.

يتضمن كل متصفح ويب أداة تسمح أو تمنع المواقع من عرض النوافذ المنبثقة عند التصفح.

حظر النوافذ المنبثقة:

> افتح برنامج **Microsoft Edge** واضغط **Settings and more** (الإعدادات والمزيد). ❶

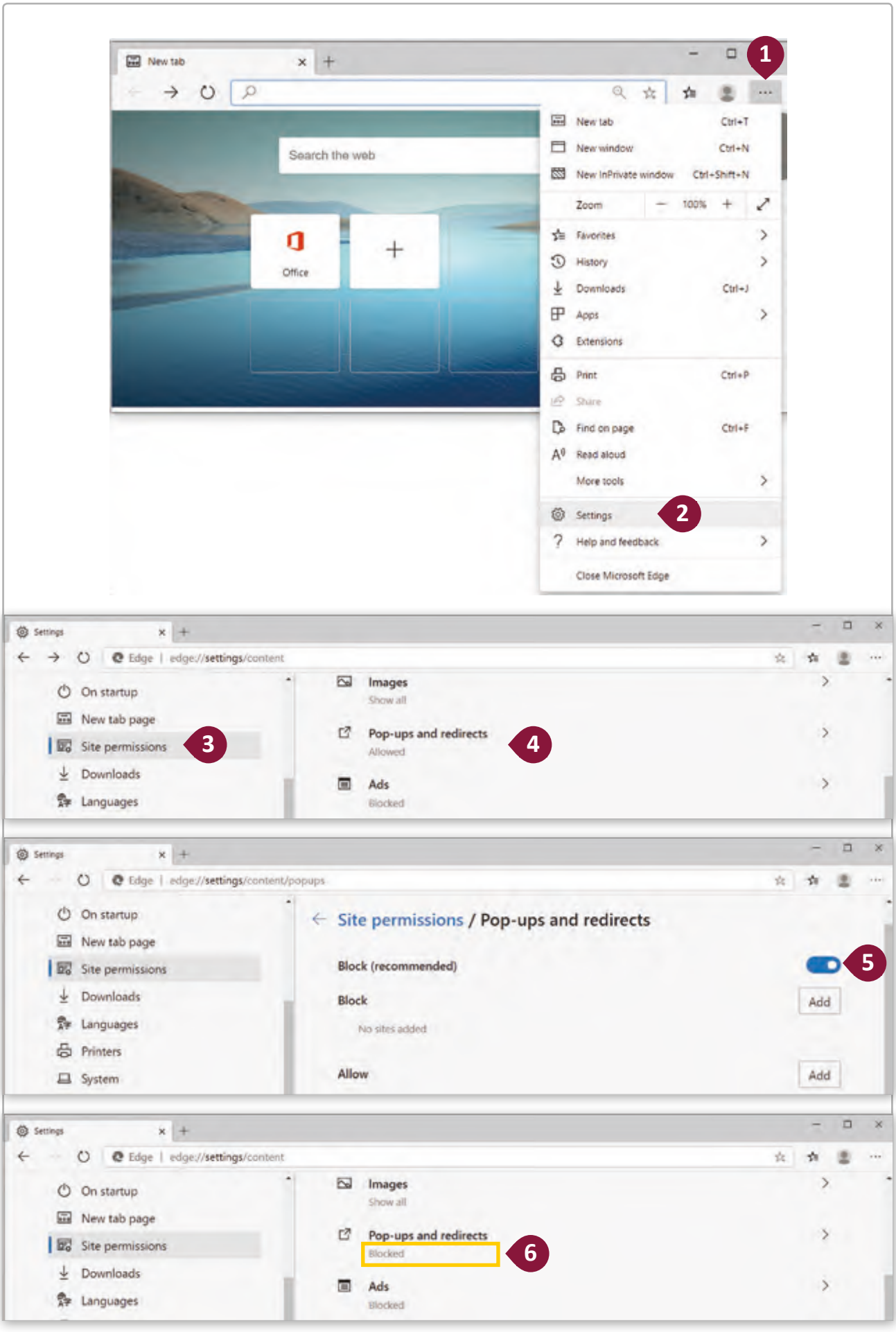
> اضغط **Settings** (الإعدادات). ❷

> اضغط **Site permissions** (أذونات الموقع). ❸

> اضغط **Pop-ups and redirects** (العناصر المنبثقة وعمليات إعادة التوجيه). ❹

> حرك زر التبديل **Block** (حظر) إلى وضع **On** (مفعل). ❺

> إن قدرة متصفح الويب على حظر النوافذ المنبثقة قد تم تفعيلها الآن. ❻


New tab
Search the web
Office
New tab Ctrl+T
New window Ctrl+N
New InPrivate window Ctrl+Shift+N
Zoom 100%
Favorites
History
Downloads Ctrl+J
Apps
Extensions
Print Ctrl+P
Share
Find on page Ctrl+F
Read aloud
More tools
Settings
Help and feedback
Close Microsoft Edge
1
2
Settings
Edge | edge://settings/content
On startup
New tab page
Site permissions
Downloads
Languages
Images
Show all
Pop-ups and redirects
Allowed
Ads
Blocked
3
4
Edge | edge://settings/content/popups
Site permissions / Pop-ups and redirects
Block (recommended)
Block
Add
No sites added
Allow
Add
Printers
System
5
Pop-ups and redirects
Blocked
6

تمكين Windows Defender SmartScreen من حظر المواقع الضارة

يحمينا **Windows Defender SmartScreen** من مواقع وتطبيقات الاحتيال الإلكتروني و من البرامج والملفات الضارة.

لا يحمي البرنامج من الملفات الضارة على مواقع الشبكة الداخلية أو مشاركات الشبكة.

لتفعيل Windows Defender SmartScreen:

> اضغط زر **Start** (ابدأ) ثم **Settings** (الإعدادات). ❶

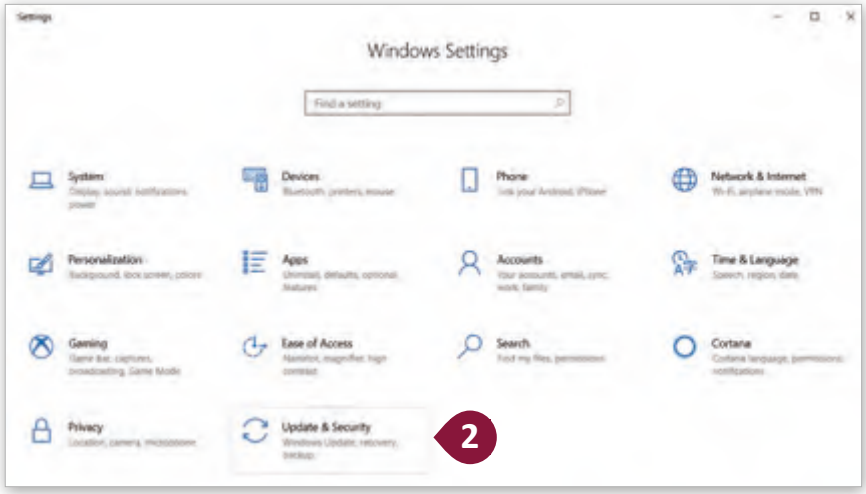
> اضغط **Update & Security** (التحديثات والأمان). ❷

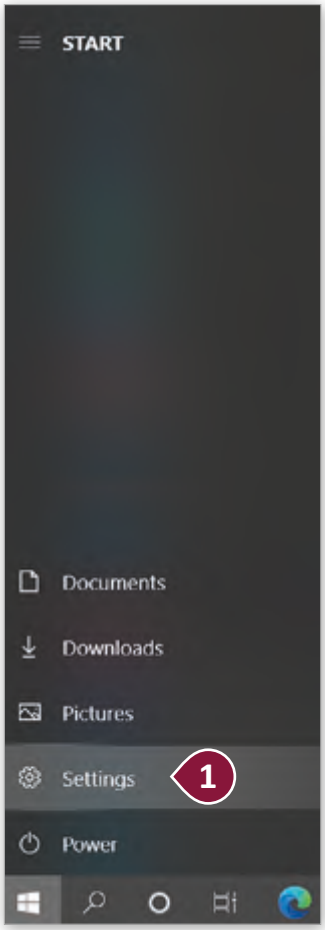
> اضغط **Windows Security** (أمان ويندوز). ❸

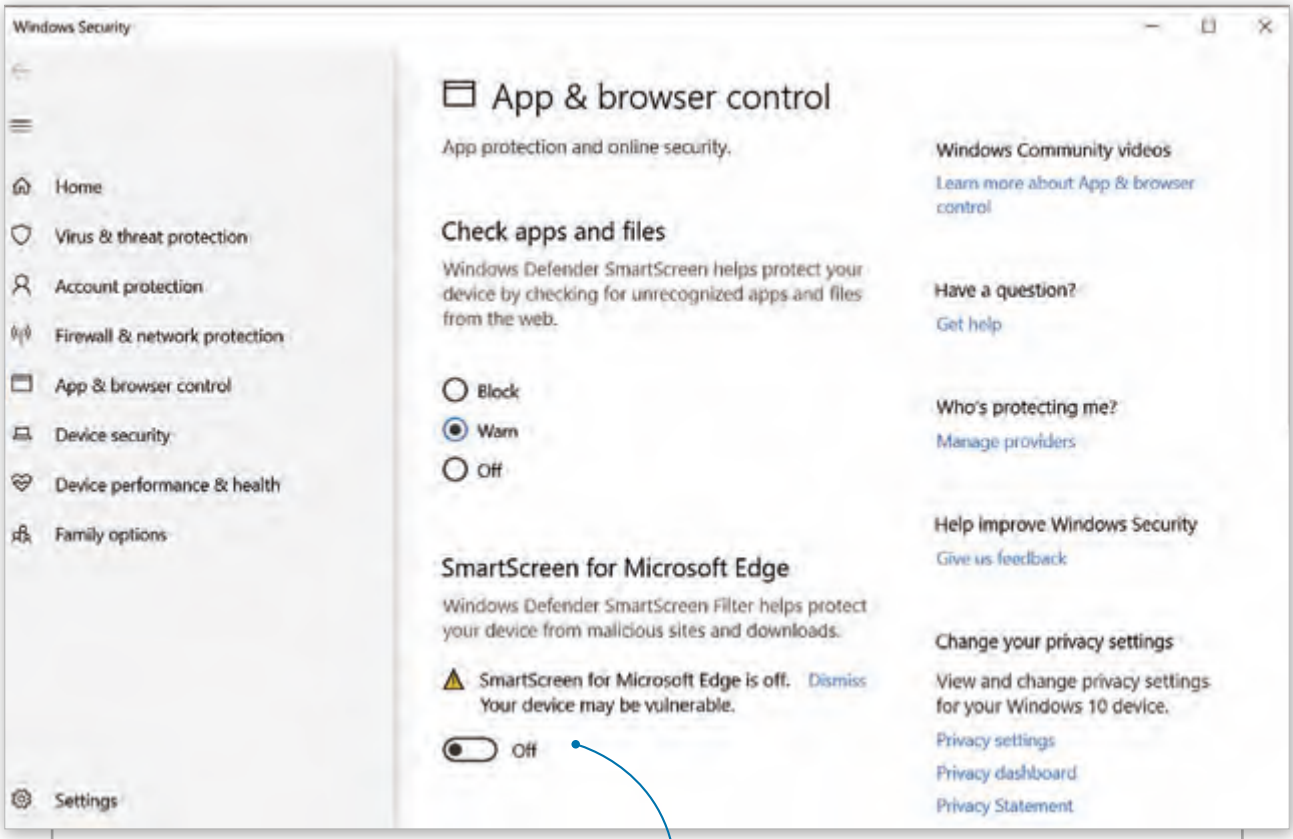
> اضغط **App & browser control** (التحكم بالمتصفح والتطبيقات). ❹

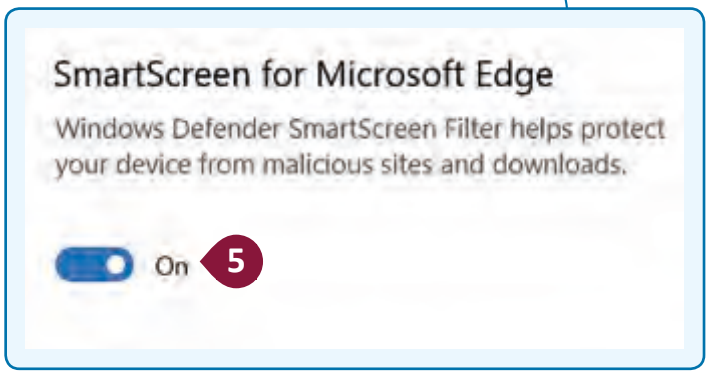
> تحت خيار **SmartScreen for Microsoft Edge** حرك الزر إلى **On**. ❺

> تم تفعيل **Windows Defender SmartScreen**. ❻






Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
App & browser control
App protection and online security.
Check apps and files
Windows Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.
Block
Warn
Off
SmartScreen for Microsoft Edge
Windows Defender SmartScreen Filter helps protect your device from malicious sites and downloads.
SmartScreen for Microsoft Edge is off. Dismiss
Your device may be vulnerable.
Off
Windows Community videos
Learn more about App & browser control
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement


SmartScreen for Microsoft Edge
Windows Defender SmartScreen Filter helps protect your device from malicious sites and downloads.
On
5


Settings
Home
Find a setting
Update & Security
Windows Update
Delivery Optimization
Windows Security
Backup
Troubleshoot
Recovery
Activation
Windows Security
Windows Security is your home to view and manage the security and health of your device.
Open Windows Security
Protection areas
Virus & threat protection
No actions needed.
Account protection
No actions needed.
Firewall & network protection
No actions needed.
App & browser control
No actions needed.
6
Device security
No actions needed.

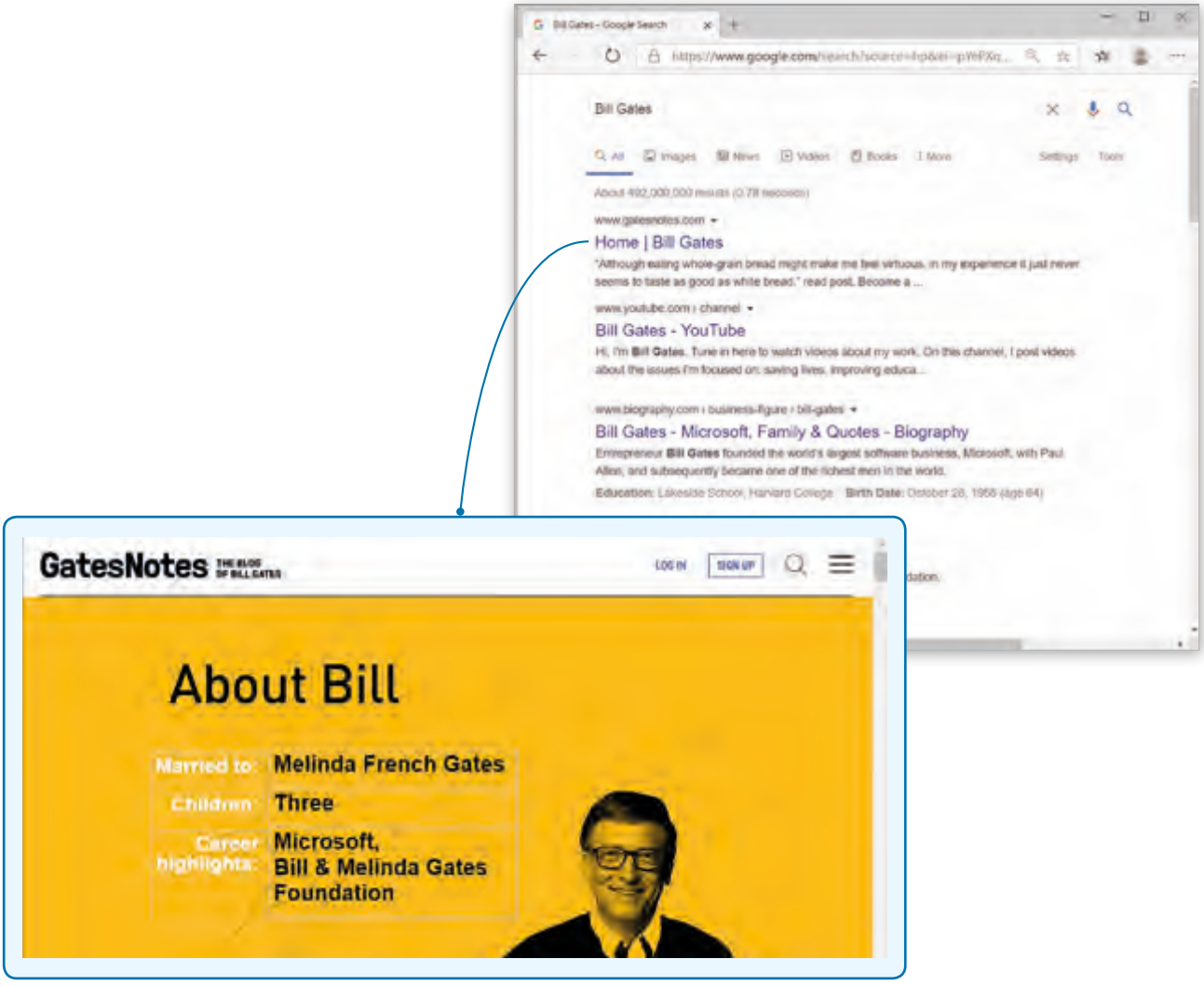
إن إحدى الفوائد المهمة لشبكة الإنترنت هي وجود كم هائل من المعلومات، ولكن هناك جانب سلبي لذلك يتمثل في أنه يُمكن لأي شخص وضع المعلومات على هذه الشبكة.

إن التحدي الأكبر عند استخدام شبكة الإنترنت لا يقتصر على العثور على الموقع المناسب الذي يحتوي على المعلومات المطلوبة، بل في وجوب التحقق من صحة المعلومات التي نعثر عليها.

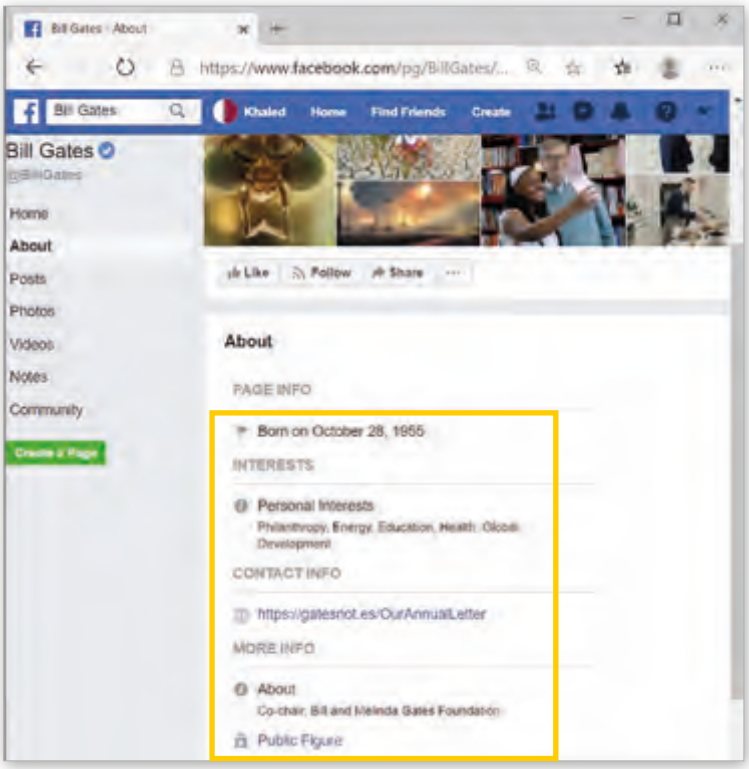
توجد العديد من الطرق للعثور على معلومات شخصية عن الأشخاص، وكل ما علينا فعله هو أن نحدد نطاق البحث عن الشخص، أو بمعنى آخر أن نعرف أين نبحث.

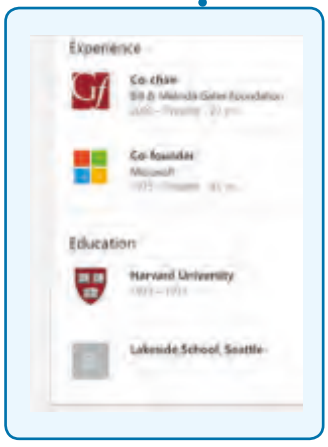
يمكن أن تتم عملية البحث من خلال كتابة الاسم بالكامل، أو كتابة اسم العائلة في إحدى محركات البحث كمحرك بحث **Google**، على سبيل المثال: **Bill Gates**، ثم يمكن تفحص نتائج البحث للعثور على صفحات ويب تحتوي المعلومات العائلية أو صفحات **Facebook** أو مواقع الصور.

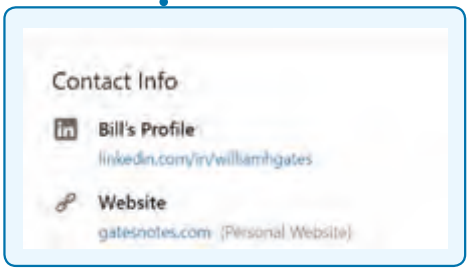
توفر نتيجة البحث هذه ثروة من المعلومات المجانية المتاحة عن أي شخص، حيث يمكن الحصول على معلومات تفصيلية بسهولة، بل يمكننا معرفة التاريخ الدراسي أو الجامعي للشخص والأصدقاء والمعتقدات والمؤثرين وحتى معلومات الاتصال.

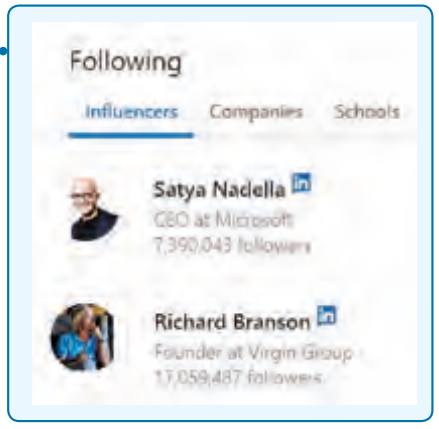


من الممكن الحصول على مصادر خاصة بالمعلومات التجارية والإنجازات الشخصية، وذلك من خلال البحث عن الشخص على مواقع التواصل الاجتماعي **Twitter** و **Facebook** و **LinkedIn**.









المعلومات الشخصية التي يجب عدم نشرها

ما ننشره عبر الإنترنت يمكن رؤيته من قبل أي شخص، وتعدُّ 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.

المعلومات الشخصية التي قد تؤثر على الحصول على وظيفة في المستقبل

إن كل ما نقوله أو نقوم بمشاركته على شبكه الإنترنت يمثل هويتنا وشخصيتنا، ولذا يجب أن نتجب نشر ما يمكن أن يشكل عقبة أمام حصولنا على وظيفة في المستقبل مثل:

- الصور غير اللائقة.
- التعليقات غير اللائقة.
- التعليقات السلبية بخصوص وظيفة سابقة أو صاحب عمل أو رئيس أو مدرس سواء حاليًا أو من الماضي.
- البيانات التي تُظهر ضعف مهارات الاتصال.
- التعليقات العنصرية.
- المؤهلات الكاذبة.
- المعلومات السرية عن عمل أو صاحب عمل سابق.
- البيانات التي تظهر ضعف المهارات الإملائية أوالنحوية.

الأخطار الناجمة عن كشف المعلومات الشخصية

إذا كنا نعتقد أن معلوماتنا الشخصية آمنة، فيجب أن نفكر مرة أخرى. لقد أصبح الحفاظ على معلوماتنا آمنة الآن هو الاستثناء وليس القاعدة.

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.

من المثير أن اللصوص يدركون أن أفضل وقت لسرقة منزلنا هو وقت عطلتنا، ويمكنهم معرفة ذلك بسهولة إذا نشرنا خطط عطلتنا على وسائل التواصل الاجتماعي.

1

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

2

وضح الخطوات الواجب عليك اتباعها من أجل تصفح اجتماعي آمن.

3

اذكر المعلومات التي يجب عليك عدم مشاركتها.

_____

_____

_____

4

صف الأخطار التي قد تتعرض لها عند تسريب معلوماتك الشخصية.

_____

_____

_____

5

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

6

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

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

اكتب فقرة تتضمن أهم ما عثرت عليه.

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

الدرس الخامس

أمن البريد الإلكتروني، الشبكة الخاصة الافتراضية VPN، وأجهزة إنترنت الأشياء IoT.

إن المهمة الأساسية لأمن تكنولوجيا المعلومات هي توفير وسائل وطرق الحماية اللازمة ضد التهديدات المحتملة. سنناقش في هذا الدرس بعض الوسائل والطرق المستخدمة في ذلك مثل الشهادات الرقمية، والتوقيع الرقمي وكيفية استخدامه لتأكيد هوية الشخص الموقِّع، وسنناقش أيضًا كيفية تأمين أجهزة إنترنت الأشياء، في النهاية سنتعلم كيفية استخدام الشبكة الافتراضية الخاصة **(VPN)** في إنشاء شبكة خاصة داخل الشبكة العامة.

مع تزايد الهجمات والجرائم الإلكترونية في فضاء الإنترنت؛ أصبحت الحاجة إلى توفير سبل الحماية أحد أهم الأولويات لدى الأفراد أو الشركات التي تمارس أعمالها على الشبكة، ولا يقتصر ذلك فقط على حماية المؤسسة أو الشركة وأسرار مهنتها من المخترقين والمتلصصين؛ وإنما يمتد ذلك إلى حماية العملاء وأجهزتهم مما يعطي الشركة مزيدًا من المصداقية ويبني جسورًا من الثقة بينها وبين عملائها.

وأحد سبل الحماية التي يستخدمها الأفراد والشركات لضمان أمن البيانات ما يسمى بـ الشهادة الرقمية **Digital Certificate** أو المعرف الرقمي **Digital ID**، وهي تكنولوجيا تشفير خاصة تمكن مستخدميها من إثبات هويتهم أثناء التواصل مع الآخرين وتؤكد صحة البيانات التي يشاركونها معهم وسلامتها من التزوير أو العبث.

يمكن للمؤسسات من خلال استخدام الشهادات الرقمية أن تحقق ما يلي:

- الالتزام بالقانون، حيث تفرض بعض الدول على المؤسسات التي تمارس التجارة الإلكترونية استخدام الشهادات الرقمية.
- الحصول على درجة عالية من الأمان.
- زيادة الثقة بين المؤسسة والعملاء.

تحتوي الشهادة الرقمية على بيانات اعتماد إلكترونية تُستخدم لتأكيد الهويات عبر الإنترنت للأفراد والمؤسسات وأجهزة الحاسوب والكيانات الأخرى على الشبكة.

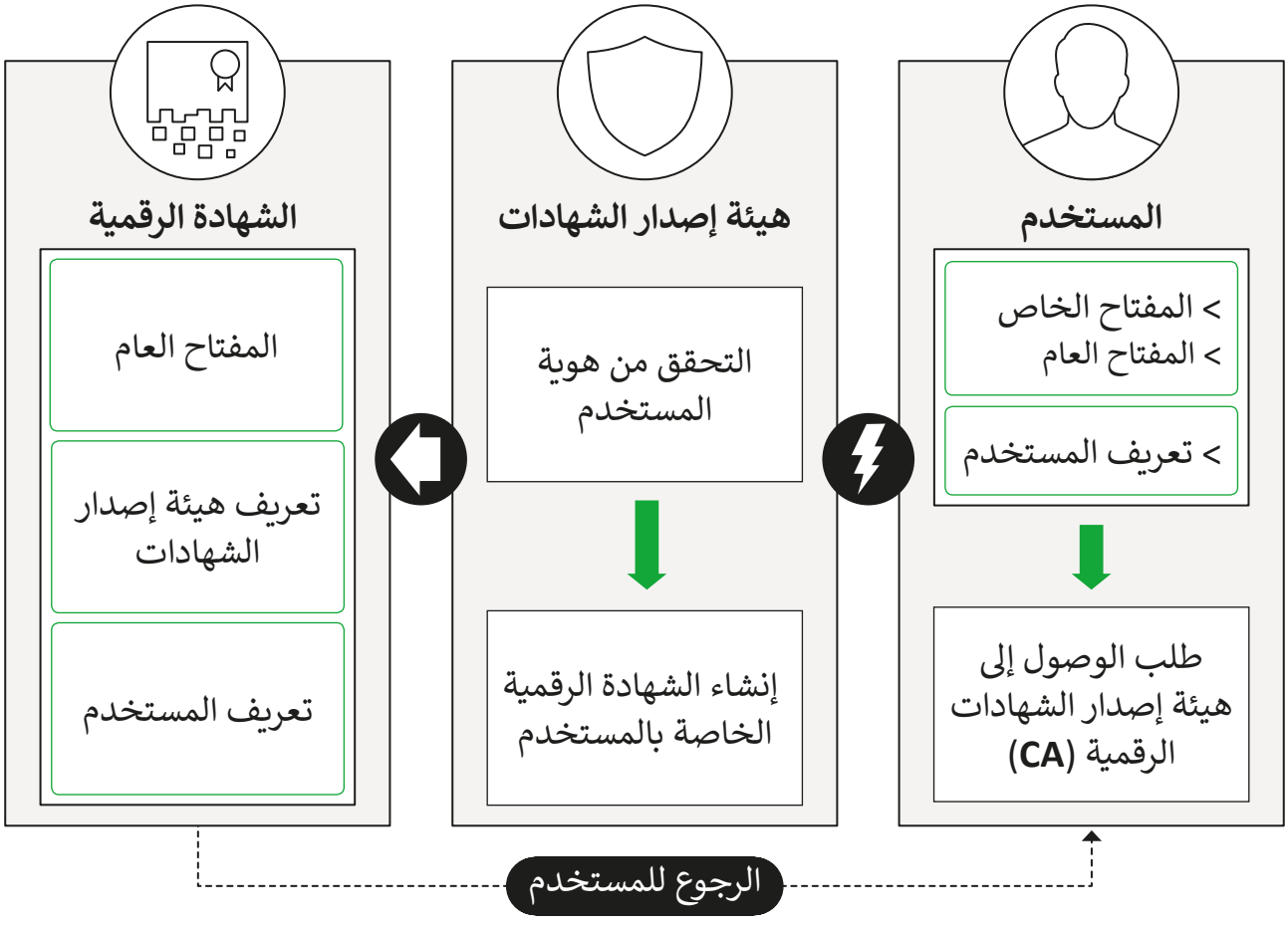
يمكن استخدام الشهادات الرقمية في مجموعة متنوعة من المعاملات الإلكترونية بما في ذلك البريد الإلكتروني، والتجارة الإلكترونية وبرامج العمل التعاوني، وكذلك لتأمين عمليات تحويل الأموال إلكترونيًا.

يتشابه عمل الشهادة الرقمية مع بطاقات التعريف الشخصية كجواز السفر مثلًا بحيث توفر معلومات كافية حول هوية الكيان الذي يحملها والذي قد يكون شخصًا أو مؤسسةً أو جهازًا إلكترونياً.

إصدار الشهادة الرقمية

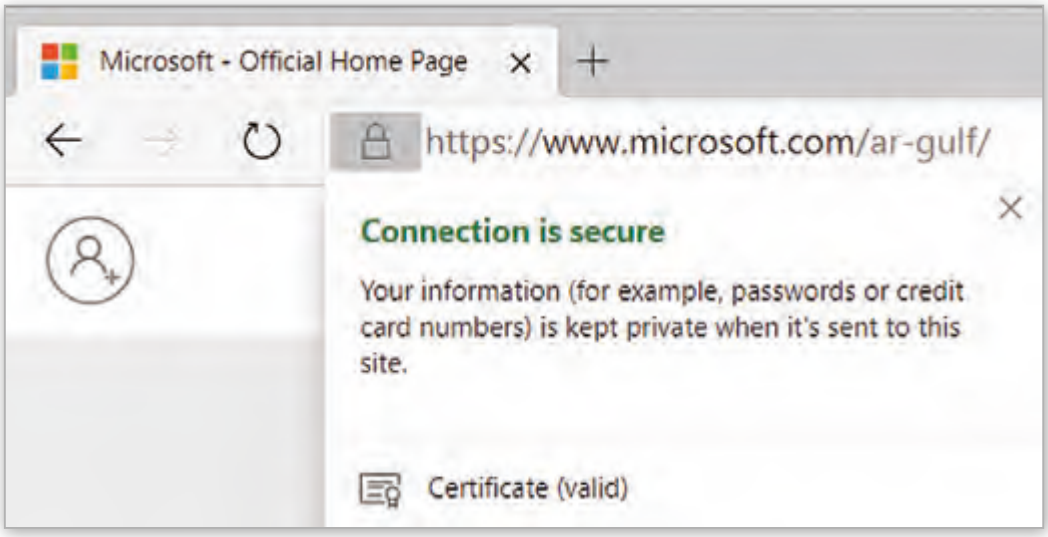
يتم إصدار هذه الشهادات الرقمية من قبل هيئة مخولة بإصدار الشهادات تسمى **Certificate Authority (CA)**، والتي تضمن بدورها صلاحية المعلومات الواردة في الشهادة. تعمل هذه الهيئات كمرجعيات أو كطرف ثالث موثوق به من قبل كل من مالك الشهادة والطرف المعتمِد على الشهادة. توجد العديد من هيئات إصدار الشهادات الموثقة حول العالم، كما وتقوم العديد من المؤسسات والحكومات والشركات بإصدار شهاداتها الخاصة. من أمثلة هيئات إصدار الشهادات الموثقة في جميع أنحاء العالم **Verisign** و**Entrust** و**GlobalSign** و**IdenTrust** وغيرها.

عندما يطلب شخص ما شهادة رقمية، تتحقق الجهة المسؤولة من هوية مقدم الطلب ومن استيفائه لجميع متطلبات الحصول عليها، ثم يتم إصدار الشهادة على شكل ملف حاسوب.

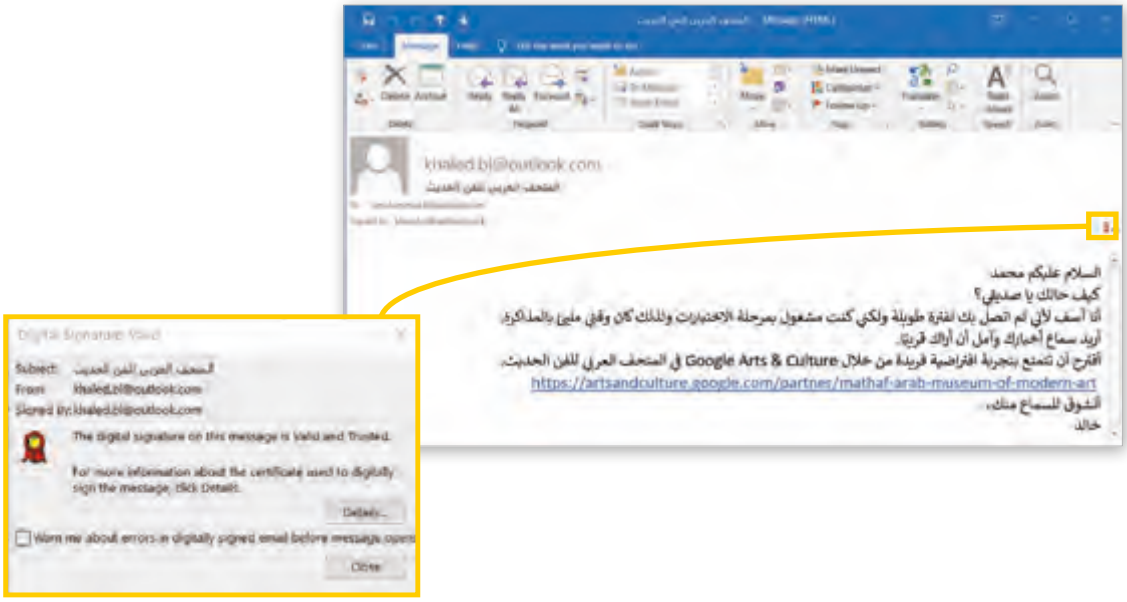


يمكن للمؤسسة بعد حصولها على الشهادة الرقمية استخدامها في مختلف المعاملات الإلكترونية، مثلًا في تبادل رسائل البريد الإلكتروني مع العملاء والموردين وغيرهم، أو في المتاجر الإلكترونية الخاصة بهم، أو عند إجراء عمليات تحويل الأموال الإلكترونية.

يمكننا كمستخدمين التعرف على وجود مثل هذه الشهادة في مواقع الويب الخاصة بالمؤسسات، حيث يمكن ملاحظة وجود رمز القفل قبل الاختصار "**https**" في الجزء الأيسر من عنوان **URL** لموقع الويب المحمي بشهادة وذلك عند استعراض ذلك الموقع من خلال المتصفح، كما يمكننا ضغط رمز القفل لعرض محتويات الشهادة.



تستخدم الشهادات الرقمية كذلك في البريد الإلكتروني، حيث يتم توقيع الرسائل الإلكترونية باستخدام الشهادة الرقمية لإثبات هوية المرسل، يمكن للمستلم رؤية رمز شهادة صغير في الرسالة، عندما يضغط المستلم على الرمز، يتم عرض اسم المرسل وعنوان البريد الإلكتروني وموضوع البريد الإلكتروني الأصلي.



توفر الشهادة الرقمية مزايا الأمان التالية:

- تحتوي على معلومات شخصية للمساعدة في التعرف على مالك الشهادة وتعقبه.
- تحتوي على المعلومات المطلوبة لتحديد والاتصال بالهيئة أو المؤسسة التي قامت بإصدار تلك الشهادة.
- يتم تصميم هذه الشهادة بشكل يمنع التزييف والتزوير.
- يمكن للهيئة أو المؤسسة التي قامت بإصدار الشهادة أن تقوم بإلغائها في حالات معينة كحالة إساءة استخدام الشهادة أوسرقتها.

يحصل الموظفون على شهاداتهم الرقمية عادة من مكان العمل. قم بالبحث عن الشركات التي تصدر الشهادات الرقمية.

المعرف الرقمي Digital ID

يرتبط المعرف الرقمي بالشهادة الرقمية، ويعد ضروريًا للقيام بعمليات التوقيع الرقمي حيث يوفر المفتاح العام (**Public Key**) الذي يمكن استخدامه للتحقق من صحة المفتاح الخاص (**Private Key**) المرتبط بالتوقيع الرقمي. عادةً ما يحتوي المعرّف الرقمي على الاسم وعنوان البريد الإلكتروني واسم الهيئة أو المؤسسة التي أصدرته والرقم التسلسلي وتاريخ انتهاء الصلاحية.

تحتوي المعرفات الرقمية على مفتاحين:

- المفتاح العام **Public Key** الذي يقفل البيانات أو يشفرها.
- والمفتاح الخاص **Private Key** الذي يفتح أو يفك تشفير تلك البيانات.

إذا أردنا تبادل رسائل بريد إلكتروني موقعة رقميًا، وأردنا أن يتمكن مستلمو تلك الرسائل من التحقق من صحة التوقيع الرقمي الخاص بنا، يجب علينا استيراد ملف المعرف الرقمي في تطبيق البريد الإلكتروني الذي نستخدمه، على سبيل المثال **Microsoft Outlook**.

لاستيراد معرف رقمي موجود مسبقًا:

> افتح **Microsoft Outlook** ومن علامة تبويب **File** (ملف)، اضغط **Options** (خيارات). ❶

> اضغط **Trust Center** (مركز الثقة) ❷ ومن **Microsoft Outlook Trust Center** اضغط **Trust Center Settings** (إعدادات مركز الثقة). ❸

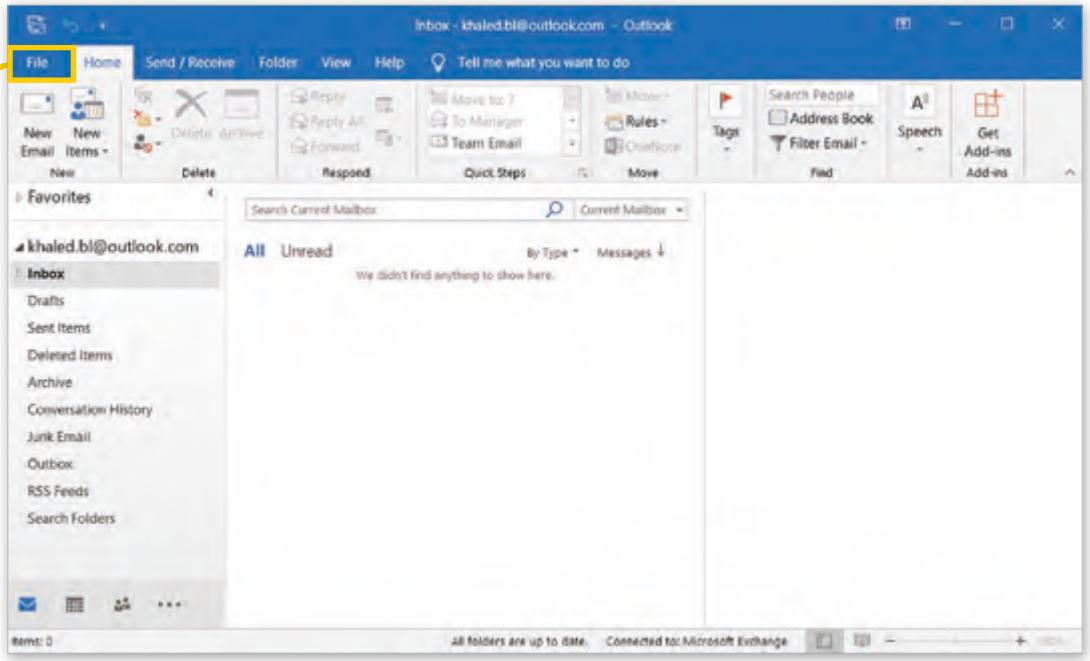
> اضغط **Email Security** (أمن البريد الإلكتروني). ❹ ومن **Digital IDs (Certificates)** اضغط **Import/Export** (استيراد / تصدير). ❺

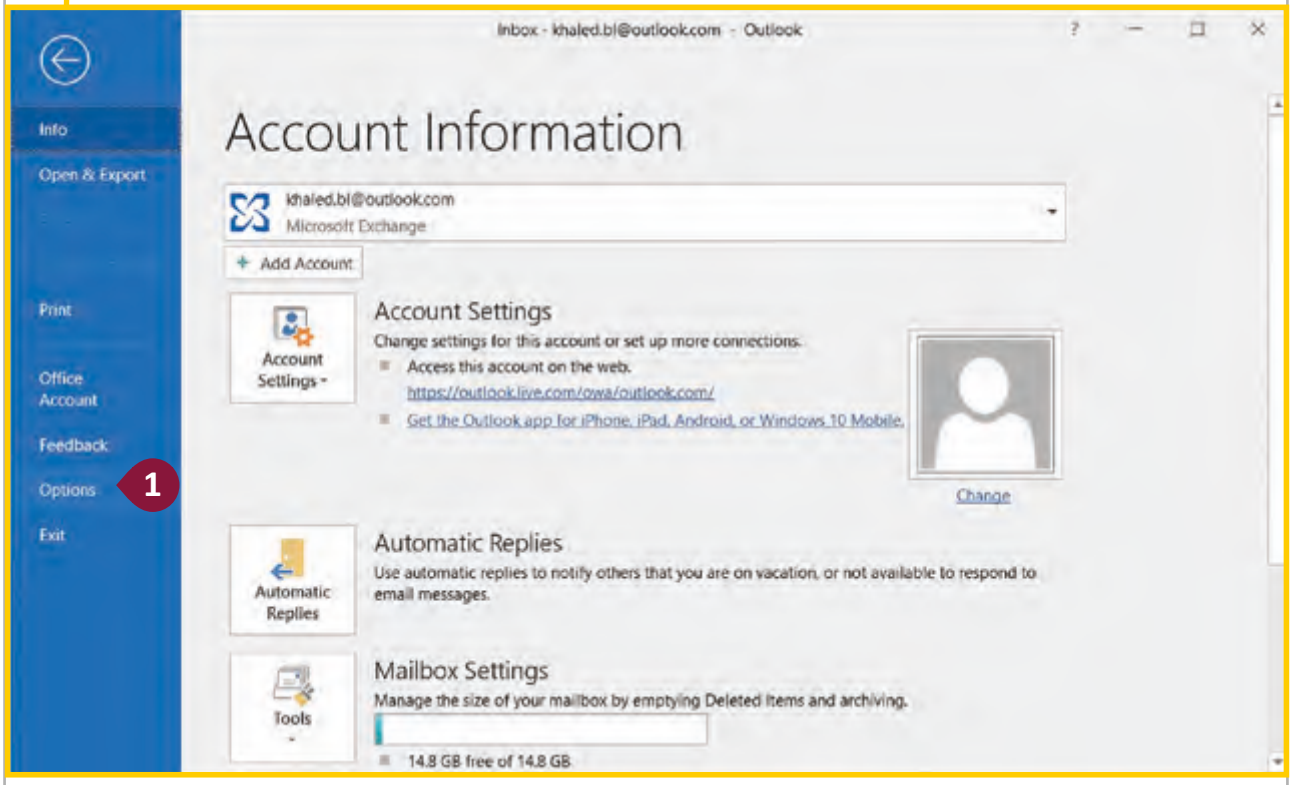
> اختر **Import existing Digital ID from a file** (استورد معرف رقمي موجود من ملف) واضغط **Browse** (استعراض). ❻

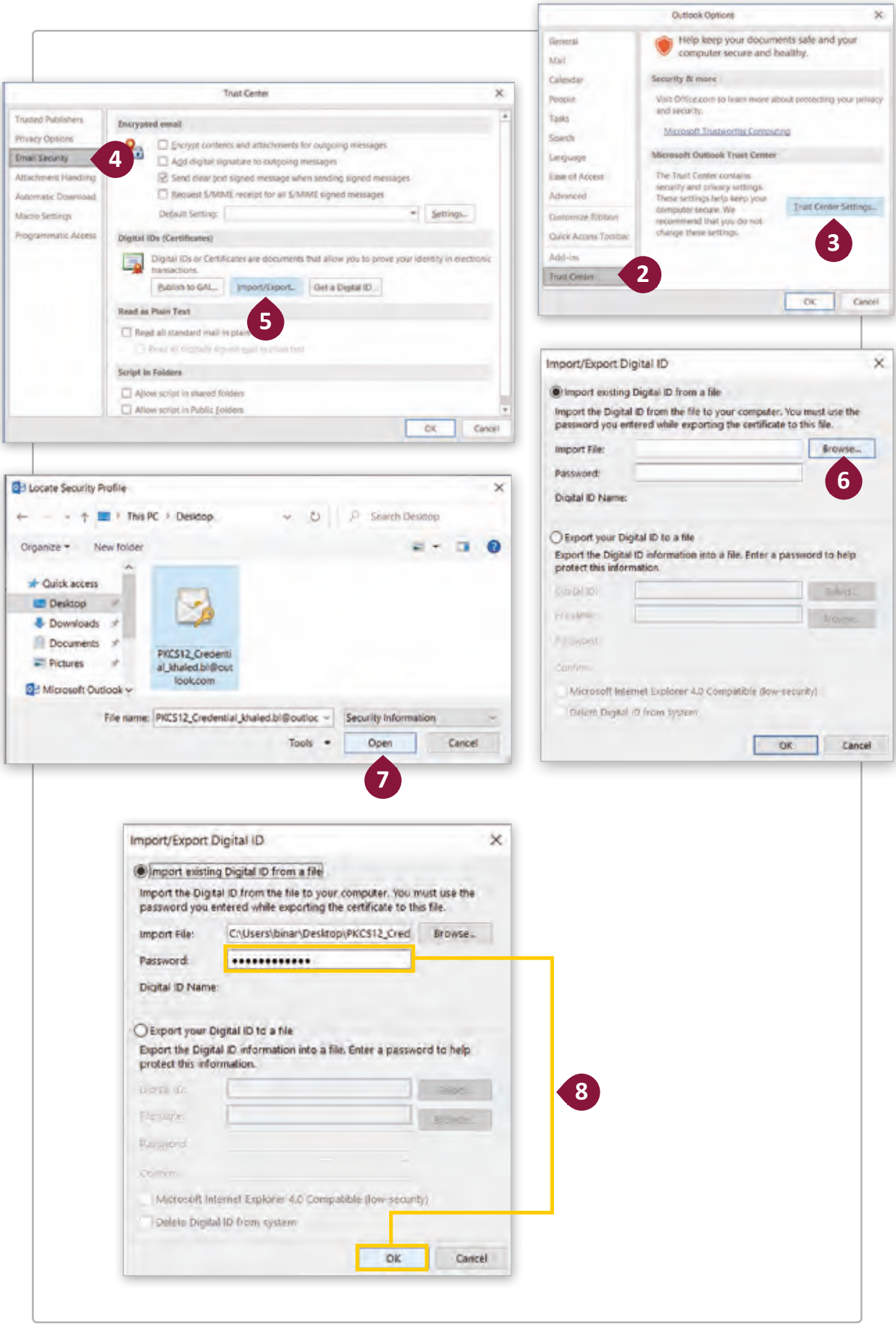
> حدد ملف المعرف الرقمي ثم اضغط **Open**. ❼

> اكتب كلمة المرور التي تم تزويدك بها من مزود المعرف الرقمي واضغط **OK** (تم). ❽

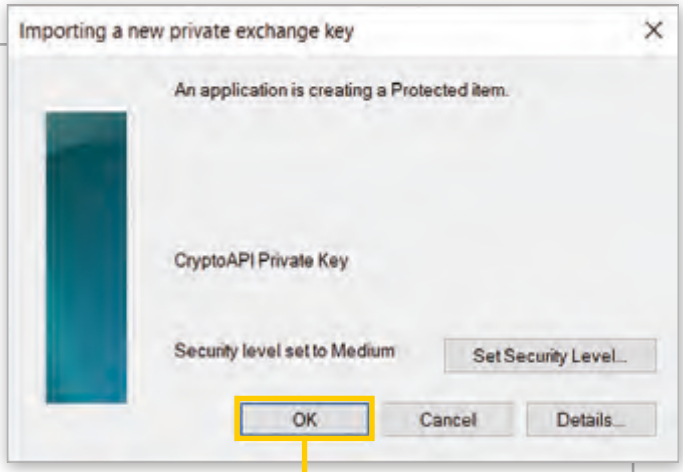
> من نافذة **Import/Export Digital ID** (استيراد/تصدير المعرف الرقمي) وفي النوافذ الأخرى المفتوحة اضغط **OK** (تم). ❾

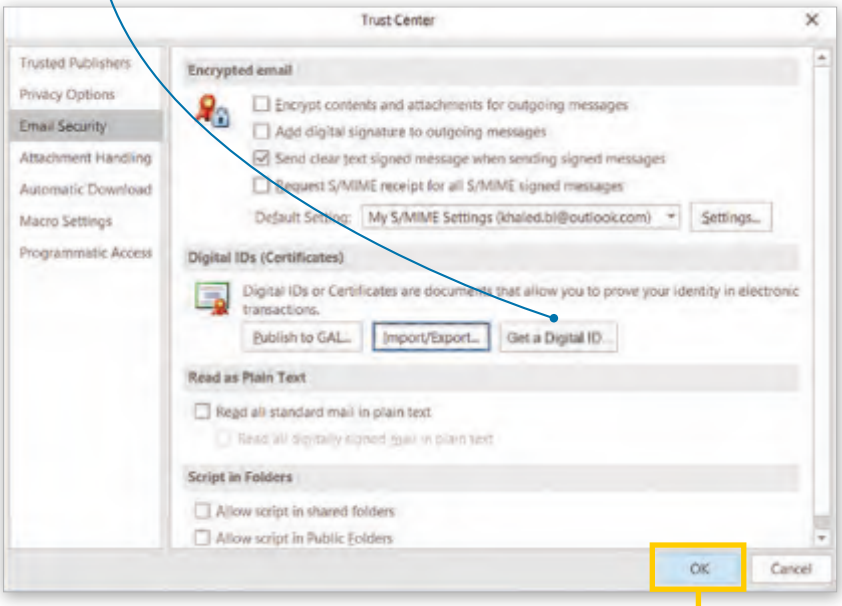

Inbox - khaled.bl@outlook.com - Outlook
File
Home
Send / Receive
Folder
View
Help
Tell me what you want to do
New Email
New Items
Delete
Respond
Quick Steps
Move
Tags
Search People
Address Book
Filter Email
Find
Speech
Get Add-ins
Add-ins
Favorites
khaled.bl@outlook.com
Inbox
Drafts
Sent Items
Deleted Items
Archive
Conversation History
Junk Email
Outbox
RSS Feeds
Search Folders
All
Unread
We didn't find anything to show here.
All folders are up to date.
Connected to: Microsoft Exchange


Inbox - khaled.bl@outlook.com - Outlook
Info
Open & Export
Print
Office Account
Feedback
Options
1
Exit
Account Information
khaled.bl@outlook.com
Microsoft Exchange
Add Account
Account Settings
Account Settings
Change settings for this account or set up more connections.
Access this account on the web.
https://outlook.live.com/owa/outlook.com/
Get the Outlook app for iPhone, iPad, Android, or Windows 10 Mobile.
Change
Automatic Replies
Automatic Replies
Use automatic replies to notify others that you are on vacation, or not available to respond to email messages.
Tools
Mailbox Settings
Manage the size of your mailbox by emptying Deleted Items and archiving.
14.8 GB free of 14.8 GB

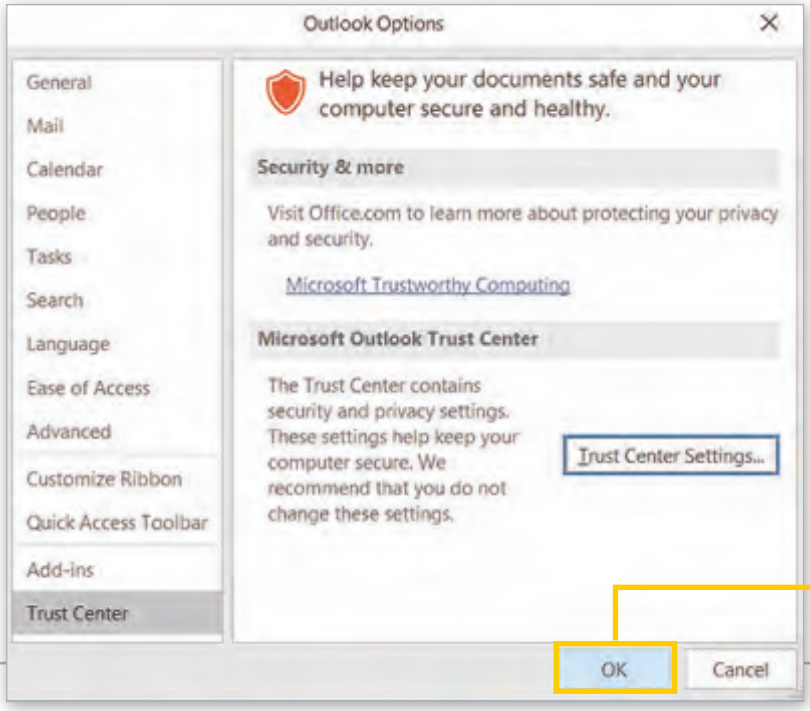

Outlook Options
Trust Center
Import/Export Digital ID
Locate Security Profile
Import/Export Digital ID
2
3
4
5
6
7
8
OK
Cancel
Browse...
Import/Export...
Trust Center Settings...

اضغط **Get a Digital ID** (الحصول على معرف رقمي) للوصول إلى قائمة من مصدري المعرفات الرقمية المناسبة لاستخدامك.





9



التوقيع الرقمي Digital Signature

لا يحتوي نظام البريد الإلكتروني - دون امتلاك شهادة رقمية - على أي طرق للتحقق من صحة البيانات المحتواة في الرسالة بما في ذلك مصدرها، كما لا يمكن التأكد ما إذا قام أي شخص بتغيير محتوى رسالة البريد الإلكتروني أثناء نقلها رقميًا من المرسل إلى المستلم، ولكن عند استخدام التوقيع الرقمي يمكن المصادقة على المعلومات الرقمية من خلال طرائق تشفير الحاسوب المستخدمة.

توفر الشهادة الرقمية لمستخدميها معرفًا رقميًا وذلك للتمكن من توقيع رسائل البريد الإلكتروني أو المستندات رقميًا بواسطة التوقيع الرقمي الخاص بصاحب الشهادة.

تفعيل زر توقيع الرسالة رقميًا:

> أنشئ رسالة بريد إلكتروني جديدة، ثم ومن نافذة الرسالة الجديدة، ومن علامة تبويب **Options** (خيارات)، وفي مجموعة **More Options** (خيارات إضافية)، اضغط **Message Options** (خيارات الرسالة). ❶

> من نافذة **Properties** (خصائص)، ومن **Security** (الأمان)، اضغط **Security Settings** (إعدادات الأمان). ❷

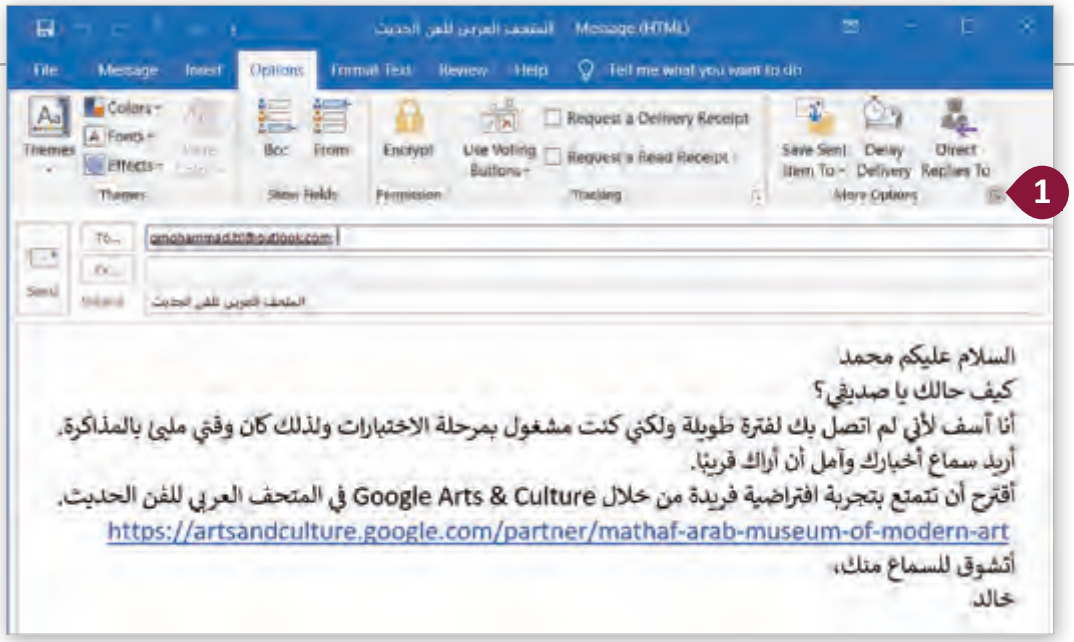
> من نافذة **Security Properties**، اختر **Add digital signature to this message** (أضف توقيعًا رقميًا إلى هذه الرسالة). ❸

> اضغط **OK** (تم). ❹

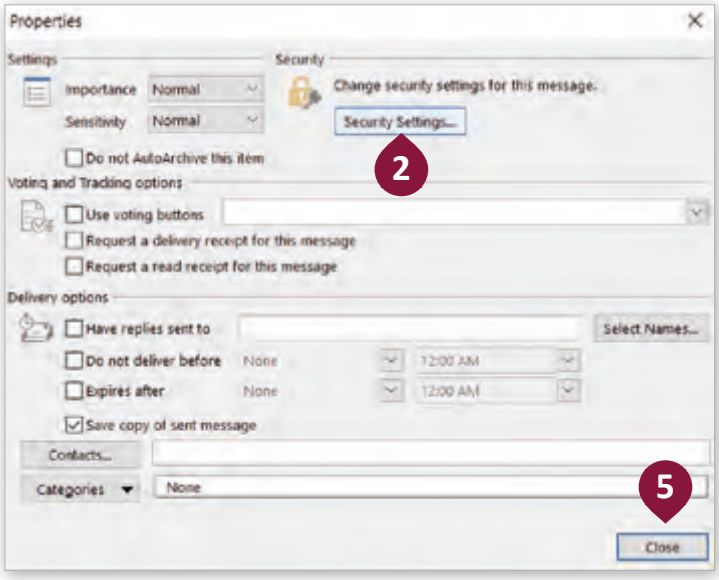
> اضغط **Close** (إغلاق). ❺

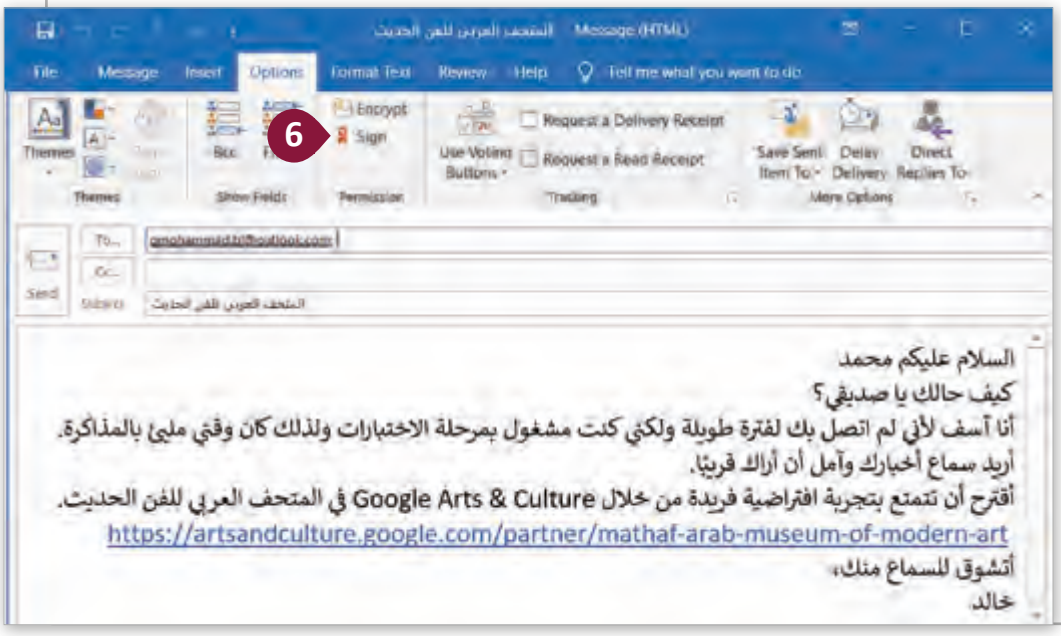
> سيظهر زر **Sign** (التوقيع). ❻

إذا لم يكن زر توقيع الرقمي ظاهرًا لديك، فهذا يعني أنه ليس لديك معرف رقمي نشط تم تكوينه لحساب بريدك الإلكتروني. عندها عليك الحصول على شهادة توقيع البريد الإلكتروني من مزود خدمة معتمد.


Message (HTML)
File
Message
Insert
Options
Format Text
Review
Help
Tell me what you want to do
Themes
Colors
Fonts
Effects
Bcc
From
Encrypt
Use Voting Buttons
Request a Delivery Receipt
Request a Read Receipt
Save Sent Item To
Delay Delivery
Direct Replies To
More Options
1
Send
السلام عليكم محمد
كيف حالك يا صديقي؟
أنا آسف لأني لم اتصل بك لفترة طويلة ولكني كنت مشغول بمرحلة الاختبارات ولذلك كان وقتي مليئ بالمذاكرة.
أريد سماع أخبارك وآمل أن أراك قريبًا.
أقترح أن تتمتع بتجربة افتراضية فريدة من خلال Google Arts & Culture في المتحف العربي للفن الحديث.
https://artsandculture.google.com/partner/mathaf-arab-museum-of-modern-art
أتشوق للسماع منك،
خالد


Security Properties
Encrypt message contents and attachments
Add digital signature to this message
3
Send this message as clear text signed
Request S/MIME receipt for this message
Security Settings
Security setting:
Change Settings...
Security Label
Policy
<None>
4
OK
Cancel

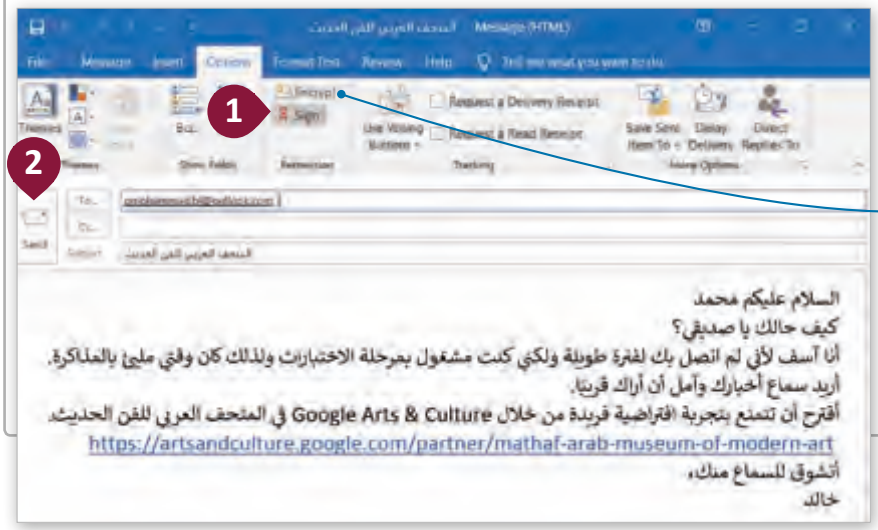

Properties
Settings
Security
Importance
Normal
Sensitivity
Normal
Change security settings for this message.
Security Settings...
2
Do not AutoArchive this item
Voting and Tracking options
Use voting buttons
Request a delivery receipt for this message
Request a read receipt for this message
Delivery options
Have replies sent to
Select Names...
Do not deliver before
None
12:00 AM
Expires after
None
12:00 AM
Save copy of sent message
Contacts...
Categories
None
5
Close


Message (HTML)
File
Message
Insert
Options
Format Text
Review
Help
Tell me what you want to do
Themes
Bcc
6
Encrypt
Sign
Use Voting Buttons
Request a Delivery Receipt
Request a Read Receipt
Save Sent Item To
Delay Delivery
Direct Replies To
Send
السلام عليكم محمد
كيف حالك يا صديقي؟
أنا آسف لأني لم اتصل بك لفترة طويلة ولكني كنت مشغول بمرحلة الاختبارات ولذلك كان وقتي مليئ بالمذاكرة.
أريد سماع أخبارك وآمل أن أراك قريبًا.
أقترح أن تتمتع بتجربة افتراضية فريدة من خلال Google Arts & Culture في المتحف العربي للفن الحديث.
https://artsandculture.google.com/partner/mathaf-arab-museum-of-modern-art
أتشوق للسماع منك،
خالد

لتوقيع رسالة بريد إلكتروني رقميًا:

> أنشئ رسالة بريد إلكتروني جديدة، ومن نافذة رسالة البريد الإلكتروني اضغط علامة تبويب **Options** (خيارات)، ومن مجموعة **Permission** (الأذن)، اضغط **Sign** (توقيع). ❶

> اضغط **Send** (إرسال). ❷



اضغط **Encrypt** (تشفير) لحماية المعلومات التي يحتمل أن تكون حساسة وذلك لحمايتها من ا لمتلصصين .

يمكنك كذلك ضبط إعدادات **Microsoft Outlook** بحيث يتم توقيع جميع الرسائل الإلكترونية رقميًا قبل إرسالها، وإليك الخطوات:

لتوقيع جميع رسائل البريد الإلكتروني رقميًا:

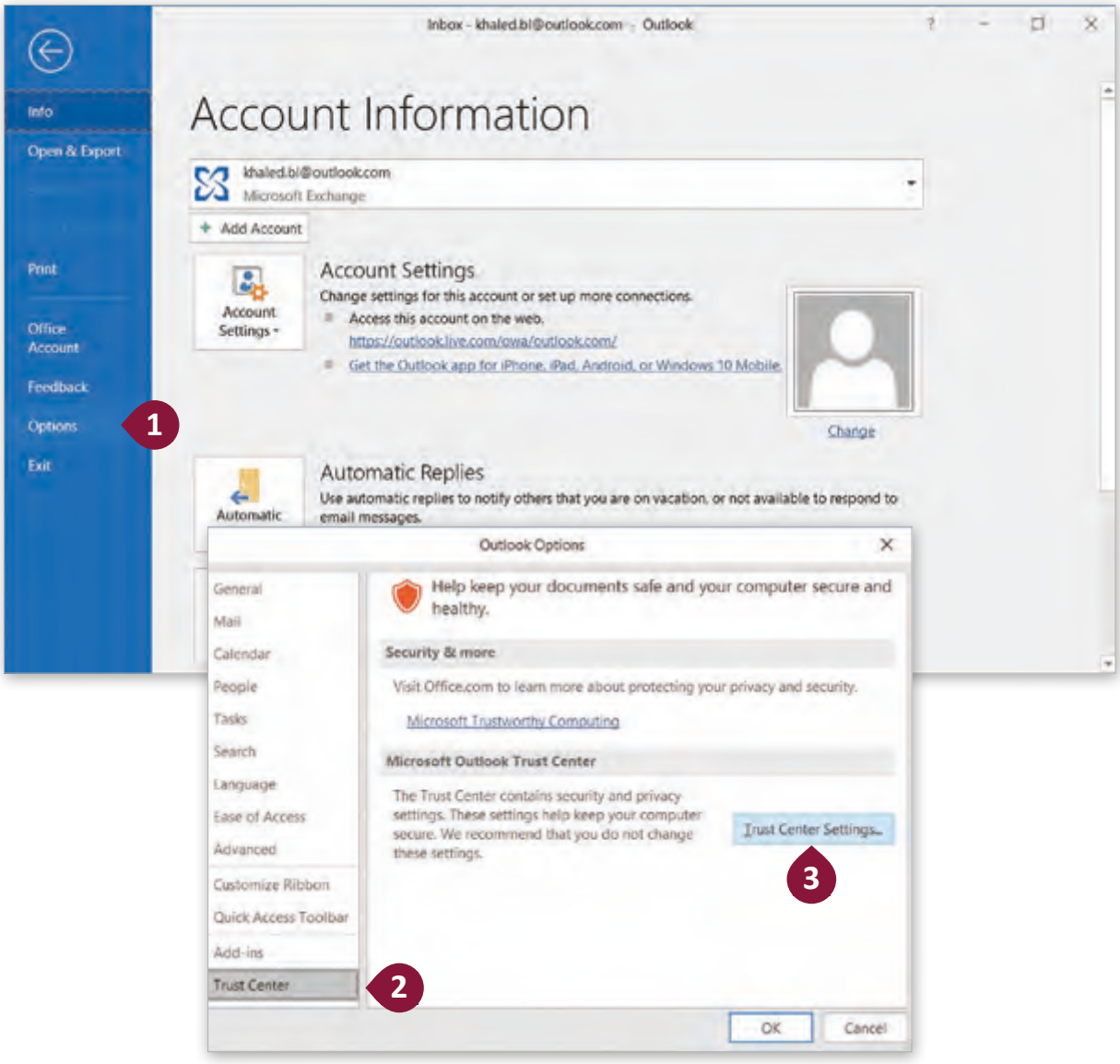
> من نافذة **Microsoft Outlook**، ومن علامة تبويب **File** (ملف)، اضغط **Options** (خيارات). ❶

> من نافذة **Outlook Options** (خيارات **Outlook**)، اضغط **Trust Center** (مركز الثقة)، ❷ ومنه اضغط **Trust Center Settings** (إعدادات مركز الثقة). ❸

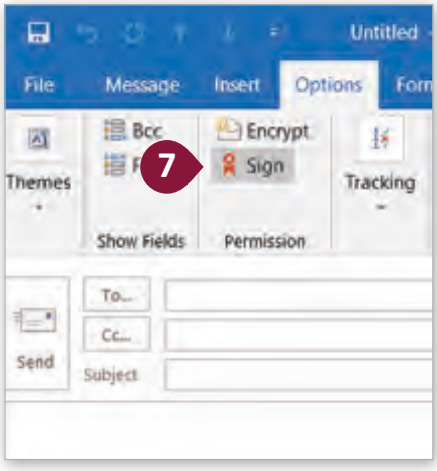
> من نافذة **Trust Center**، اضغط **Email Security** (أمان البريد الإلكتروني). ❹ ومن **Encrypted email** (البريد الإلكتروني المُشفر)، اضغط **Add digital signature to outgoing messages** (إضافة توقيع رقمي للرسائل الصادرة). ❺

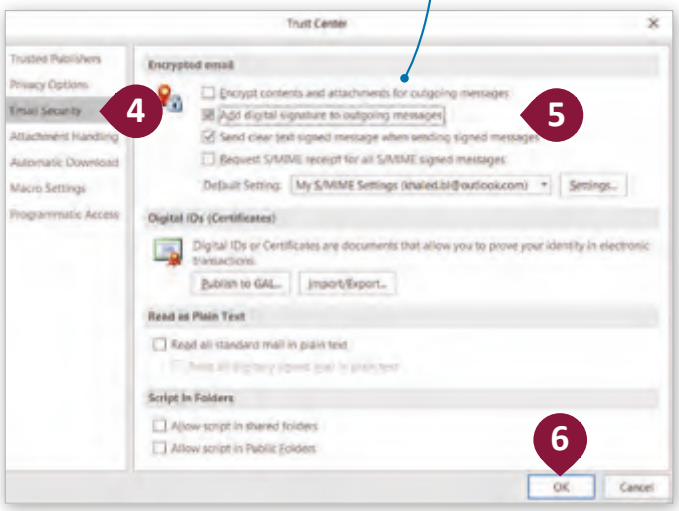
> اضغط **OK** (تم) في النوافذ الأخرى المفتوحة. ❻

> أنشئ رسالة بريد إلكتروني جديدة ولاحظ أن زر **Sign** (توقيع) قد تم تفعيله تلقائيًا. ❼



اضغط **Encrypt contents and attachments for outgoing messages** (تشفير المحتوى والمرفقات للرسائل الصادرة) لتشفير الرسائل الصادرة بصورة تلقائية.





الشبكة الافتراضية الخاصة Virtual Private Network (VPN)

الشبكة الافتراضية الخاصة (**VPN**) هي شبكة تقوم بتشفير البيانات أثناء انتقالها من موقع إلى آخر عبر شبكة الإنترنت.

تعتبر هذه الطريقة شائعة الاستخدام، حيث تسمح للمستخدمين بالوصول الآمن إلى الموارد عن بُعد، وخاصة بعد ازدياد الحاجة إلى عمل الموظفين عن بعد من منازلهم، مما يعني حاجة المؤسسات إلى تأمين وصول فعال وآمن لموظفيها عن بُعد.

يمكن للموظف من خلال استخدام الشبكة الافتراضية الخاصة أن يتصل بشكل آمن بخوادم المؤسسة دون القلق من اعتراض بيانات دخول المستخدم أو البيانات الحساسة وذلك في حالة عمله من منزله أو أي مكان خارج مبنى المؤسسة.

بعض ميزات وتحديات شبكة VPN

الميزات

- تخفي شبكات **VPN** عنوان **IP** الخاص بالمستخدم أثناء اتصاله بها، ويؤدي ذلك إلى توجيه أي هجمات محتملة من المخترقين إلى الخوادم الآمنة الخاصة بمزود خدمة **VPN** بدلًا من جهاز المستخدم.
- يؤمن استخدام شبكة **VPN** البيانات والأجهزة أثناء الاتصال بشبكات **Wi-Fi** العامة المتوفرة في الأسواق والمطارات والمواصلات العامة وغيرها.
- يضمن استخدام شبكات **VPN** تشفير الرسائل التي يقوم المستخدم بإرسالها عبر الشبكة من مختلف تطبيقات المحادثة، كما يؤمن كذلك الاتصالات الصوتية التي يقوم بها المستخدم من خلال تلك التطبيقات عبر تقنية **VoIP**.
- يسهل استخدامها عملية مشاركة الملفات والتواصل بين الموجهات البعيدة للشركات، مما يمكّن الشركات متعددة الجنسيات من إدارة أعمالها من مواقع مختلفة وتمكين الموظفين الموزعين جغرافيًا حول العالم من الوصول للبيانات المهمة بسهولة وأمان.

التحديات

- قد يبطئ الاتصال بالشبكة من خلال اتصال **VPN** من سرعة الإنترنت التي يحددها مزود الخدمة وذلك لعدة عوامل كالبعد عن الخادم ونوع التشفير المستخدم، ... وغيرها.
- عملية التكوين (الإعدادات) لشبكة **VPN** قد تكون صعبة، وقد يؤدي الضبط غير الصحيح إلى جعل بياناتنا عرضة لتهديدات الإنترنت المختلفة وللاختراق من قراصنة الحاسوب.
- لا تقوم شبكات **VPN** المجانية بعملية تشفير البيانات بطريقة صحيحة ومتكاملة مما قد يعرضنا للبرامج الضارة.
- رغم كونها الخيار الأفضل، تعتبر شبكات **VPN** المدفوعة مكلفة نوعاً ما.
- يقوم بعض مزودي خدمات **VPN** بتسجيل وتحليل بيانات الاستخدام للمستخدمين لأغراض مختلفة، مما يعرض خصوصياتنا للخطر.

الاتصال بشبكة VPN في نظام تشغيل Windows

يمكن لحاسوبك الذي يعمل بنظام تشغيل **Windows** الاتصال بشبكة افتراضية خاصة **VPN** سواء كان ذلك للعمل أو للاستخدام الشخصي، حيث يوفر الاتصال بشبكة **VPN** المزيد من الأمان في الوصول إلى شبكة شركتك وشبكة الإنترنت خلال التواجد في أماكن عامة أو الاتصال عن طريق شبكات غير آمنة كتلك التي نجدها في المطاعم و المطارات مثلًا.

ضبط إعدادات شبكة VPN

قبل أن تتمكن من الاتصال بشبكة **VPN**، يجب أن نقوم بضبط الإعدادات الخاصة بشبكة **VPN** على جهاز الحاسوب. أولًا يجب الاشتراك في خدمة **VPN** بواسطة مزود **VPN** موثوق به، أو الحصول على بيانات الاعتماد ومعلومات الخادم بالنسبة للموظفين من أماكن عملهم، إذا كانت تلك الخدمة متوفرة من مكان العمل. لأداء المهام التالية يلزم الاشتراك في خدمة **VPN**.

تكوين شبكة VPN الشخصية:

> اضغط زر **Start** (ابدأ) ثم اضغط **Settings** (إعدادات). ❶

> من **Windows Settings** (إعدادات ويندوز)، اضغط **Network & Internet** (الشبكة والإنترنت). ❷

> اضغط **VPN** ❸ ثم اضغط **Add a VPN connection** (إضافة اتصال **VPN**). ❹

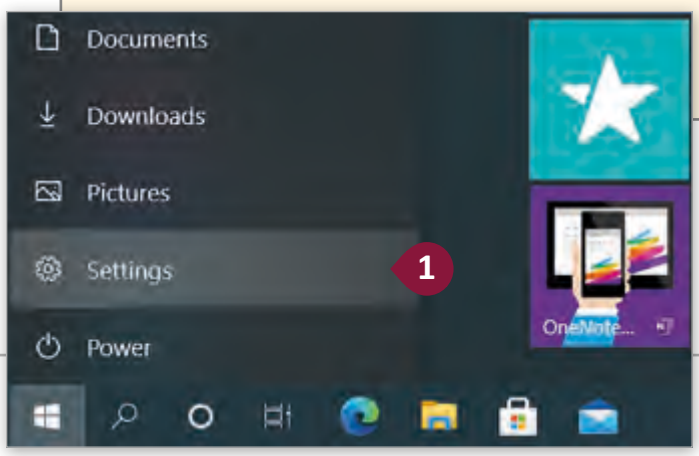
> من حقل **VPN provider** (مزود **VPN**) اختر **Windows (built in)** (مدمج في نظام **Windows**). ❺

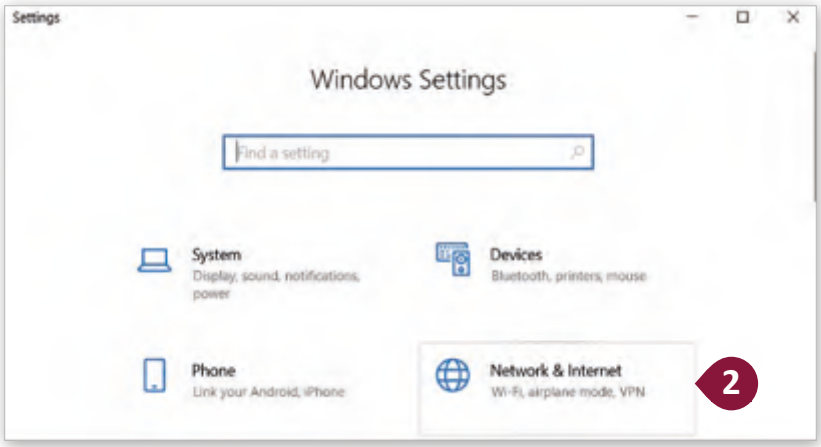
> اكتب **Connection name** (اسم الاتصال)، على سبيل المثال: **VPN**. ❻

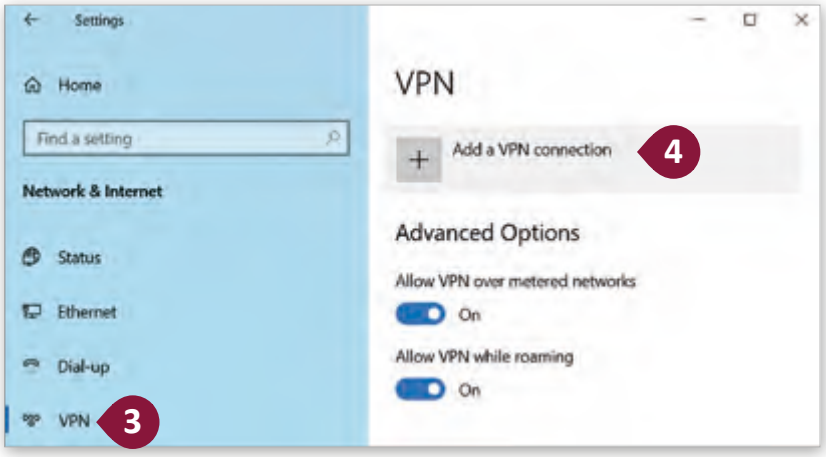
> اكتب اسم الخادم أو العنوان في حقل **Server name or address** (اسم الخادم أو العنوان). ❼

> اكتب معلومات الاتصال في حقل **Type of sign-in info** (سجل معلومات الدخول)، مثلًا: اسم المستخدم وكلمة المرور. ❽

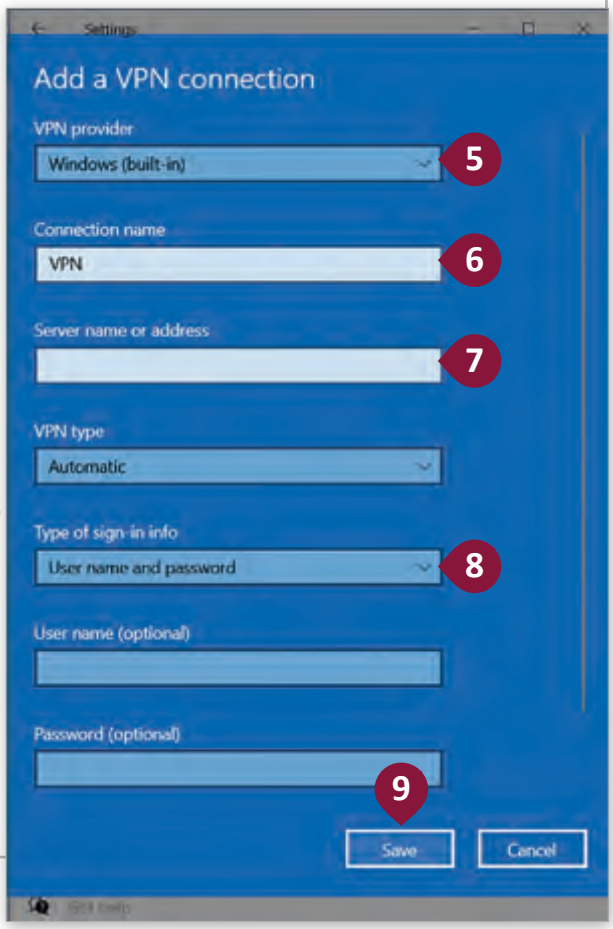
> اضغط **Save** (حفظ). ❾




Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
2


Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
3
VPN
Add a VPN connection
4
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On


Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Data usage
VPN
Add a VPN connection
VPN
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On


Settings
Add a VPN connection
VPN provider
Windows (built-in)
5
Connection name
VPN
6
Server name or address
7
VPN type
Automatic
Type of sign-in info
User name and password
8
User name (optional)
Password (optional)
9
Save
Cancel

بعد الانتهاء من ضبط إعدادات شبكة **VPN** ينبغي إجراء عملية الاتصال بها لتفعيل ميزاتها.

الاتصال بشبكة VPN:

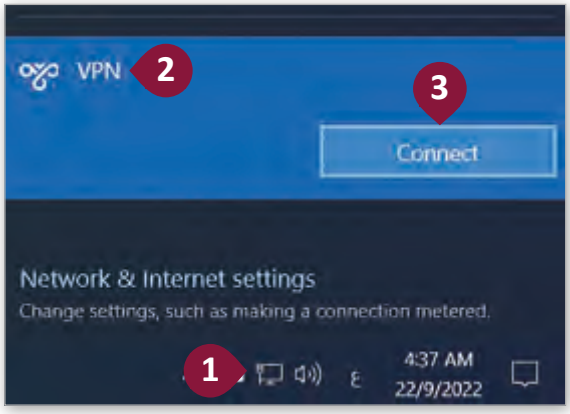
> من منطقة **Notification** (التنبيهات)، اضغط أيقونة الشبكة. ❶

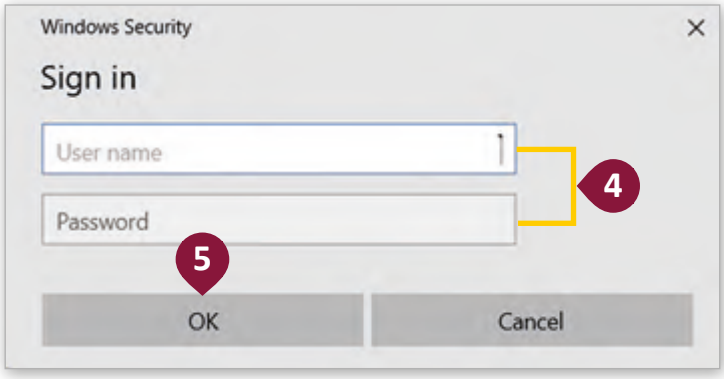
> اختر اتصال **VPN** الذي ترغب باستخدامه، واسمه في مثالنا: **VPN**. ❷

> اضغط **Connect** (اتصال). ❸

> أدخل اسم المستخدم وكلمة المرور، ❹ اضغط **OK** (تم). ❺

> عند إنشاء الاتصال، ستظهر كلمة **Connected** (متصل) أسفل اسم شبكة **VPN** التي تم الاتصال من خلالها. ❻





أجهزة إنترنت الأشياء (IoT)

تمنع شبكات **VPN** من تداول معلوماتنا الشخصية من قبل المتلصصين وبشكل خاص عند استخدام أجهزة إنترنت الأشياء في البيت أو العمل. تساعد هذه الشبكات في حماية بيانات الشركة السرية من خطر الاختراق.

تعلمت سابقًا أن أجهزة إنترنت الأشياء هي أجهزة حوسبة غير قياسية متصلة بشبكة الإنترنت ولديها القدرة على نقل البيانات. تتضمن هذه الأجهزة السماعات الذكية و أجهزة التلفاز الذكية والأجهزة القابلة للارتداء والأجهزة الذكية الأخرى. تتميز هذه الأجهزة باحتوائها على ميزات اتصال متعددة مثل **Bluetooth** وشبكة **Wi-Fi** والوصلات السلكية مثل كابلات **Ethernet**، وتمكن هذه التكنولوجيا المتقدمة مستخدميها من مراقبة أداء هذه الأجهزة والتحكم بها عن بعد عبر شبكة الإنترنت.

توجد العديد من أجهزة إنترنت الأشياء المتوافرة في الأسواق مثل:

- الهواتف الذكية.
- الثلاجات الذكية.
- الساعات الذكية.
- أجهزة إنذار الحريق الذكية.
- أقفال الأبواب الذكية.
- الدراجات الذكية.
- المستشعرات الطبية.
- متعقبات اللياقة البدنية.
- أنظمة الحماية الذكية.

أنظمة تشغيل أجهزة انترنت الأشياء (IoT OSes)

تم تصميم هذه الأنظمة لكي تتكامل مع القدرات المحدودة لأجهزة انترنت الأشياء كحجم الذاكرة وكفاءة المعالج وحجم الجهاز، مع الأخذ بالاعتبار إتاحة إمكانيات نقل البيانات والتواصل عبر شبكة الإنترنت لهذه الأجهزة.

أمثلة على أنظمة تشغيل أجهزة انترنت الأشياء:

- يعتبر **Ubuntu Core** نسخة معدلة من نظام التشغيل **Ubuntu Linux** تم إنشاؤها خصيصًا لأجهزة انترنت الأشياء.
- نظام **Fuchsia OS** هو نظام تشغيل مفتوح المصدر لأجهزة انترنت الأشياء من شركة **Google**. تم تخصيص هذا النظام ليعمل على أجهزة انترنت الأشياء وكذلك على أجهزة الحواسيب الشخصية.
- نظام **RIOT** هو نظام تشغيل مفتوح المصدر تم تخصيصه لأجهزة انترنت الأشياء، وقد تم تطوير هذا النظام من قبل مجموعة عالمية من الشركات والأكاديميين والهواة.

أوجه الاختلاف ما بين أنظمة تشغيل الحواسيب المكتبية وأنظمة تشغيل أجهزة انترنت الأشياء

	Desktop OS	IoT OS
نوع النظام	أنظمة تشغيل للأغراض العامة **General Purpose OS**	أنظمة تشغيل آنية **Real-time OS**
الغرض	تم تصميمها لتنفيذ العديد من المهام مثل التعامل مع الملفات والأجهزة، وبذلك فهي أكثر تعقيدًا.	تم تصميمها لغرض محدد وترتبط برمجياتها ومكوناتها المادية بهذا الغرض فقط.
واجهة المستخدم	تتضمن واجهة مستخدم رسومية **GUI**.	تصمم أجهزة **IoT** عادة دون شاشة أو بشاشة محدودة الإمكانيات، ولذلك يتم الوصول إلى نظام التشغيل الخاص بأجهزة **IoT** عبر واجهات الويب أو من التطبيقات في أجهزة الحاسوب أو الأجهزة الذكية الأخرى.
الوظائف	لها عديد من الوظائف، لأنه يجب أن تضمن إمكانية التشغيل التفاعلي للبرامج والأجهزة الملحقة.	لها وظائف محدودة، تنحصر في التحكم بالجهاز والإدخال والإخراج بطريقة بسيطة.

الوقت اللازم لبدء التشغيل	تستغرق وقتًا طويلًا لبدء التشغيل.	تبدأ بالتشغيل بشكل أسرع من أنظمة تشغيل الحواسيب الشخصية.
فترات التشغيل	تعمل برامجها لوقت محدد عادةً ويتم إغلاقها من قبل المستخدم.	تعمل بشكل مستمر ودائم.
استقبال المدخلات	يستقبل فقط مدخلات المستخدم، عن طريق أجهزة الإدخال المختلفة مثل الفأرة ولوحة المفاتيح، ... وغيرها.	يستقبل مدخلات المستخدم كما يستقبل مدخلات أخرى من المستشعرات الملحقة بأجهزة إنترنت الأشياء.
الأداء	تقدم تجربة أفضل للمستخدم وتمكنه من القيام بعمليات حوسبة عديدة ومعقدة وبأداء عالٍ.	تم تصميمها لكي تعمل على أجهزة صغيرة الحجم، ذات موارد حاسوبية محدودة، وتنفذ عددًا قليلًا من المهام.
المرونة	تتميز بالمرونة في قدرتها على التعامل مع الأجهزة والبرامج المختلفة وإمكانيات ترقية الأجهزة والتحكم عن بعد والحماية والتشفير، وكذلك توفر الكثير من الأجهزة الطرفية وشاشات العرض والصوت والوسائط وإمكانية تطوير البرامج الخاصة بها بشكل مستقل.	أقل مرونة، حيث تحتاج أدوات خاصة بالتطوير ولغات برمجة معينة.

المسائل المتعلقة بأمان إنترنت الأشياء

تتواصل أجهزة إنترنت الأشياء مع بعضها البعض عبر الإنترنت دون الحاجة إلى التدخل أو التوجيه من قبل المستخدم. ولأن هذه التكنولوجيا لا تزال في مهدها، فمن المحتم ظهور العديد من تحديات التصنيع والاستخدام التي ينبغي التغلب عليها لتأمين الأجهزة والمستخدمين، ومن أهم هذه التحديات:

- نقص المعرفة والخبرة لدى المستخدم.
- معايير الإنتاج غير المتسقة.
- ضعف الصيانة والتحديثات.

فيما يلي بعض أهم مخاطر استخدام إنترنت الأشياء:

اختراق أجهزة إنترنت الأشياء وبرامج الفدية:

- هذا التهديد الأمني يمكن أن يعرض السيارات ذاتية القيادة مثلًا أو المنازل الذكية أو حتى أجهزة متابعة اللياقة البدنية (القابلة للارتداء) إلى خطر حقيقي، فقد يتم إغلاق المنزل أو منع تشغيل السيارة الذكية مثلا وابتزاز أصحابها، كما يمكن أن تمنع هجمات برامج الفدية المستخدمين من الوصول إلى أجهزة إنترنت الأشياء والأنظمة الأساسية لها، بل وتعطيل تلك الأجهزة تمامًا وسرقة بيانات المستخدمين.

عدم كفاية الاختبارات ونقص التحديثات:

- يوجد نوع من التقصير من قبل الشركات المنتجة لهذه الأجهزة عندما يتعلق الأمر بإجراء الاختبارات المناسبة وتحديث البرمجيات بشكل دوري، بل وعدم اتخاذ الإجراءات الصحيحة في حالات حدوث مشكلات تتعلق بالأمان، رغم علمها أن أجهزة إنترنت الأشياء التي لا يتم تحديثها هي عرضة إلى عدد لا يحصى من البرامج الضارة وهجمات المتسللين وغيرها من الانتهاكات الأمنية.

سرقة المنازل:

- يؤدي وجود أجهزة حماية منزلية غير آمنة تعمل بتقنية إنترنت الأشياء إلى جعل تلك الأجهزة هدفًا سهلًا للاختراق من خلال معرفة عنوان **IP** الخاص بها، مما يجعل من السهل للمتسللين تحديد عنوان مستخدم الجهاز وتعريض منزله لخطر السرقة.

الوصول للمركبة الذكية عن بعد:

- قد تتعرض المركبات ذاتية القيادة أو المركبات الذكية للاختطاف وذلك من خلال اختراق أنظمتها والتحكم بها عن بعد، والإخلال بوظائف القيادة الذاتية، مما يشكل تهديدًا كبيرًا للسلامة العامة وقد يؤدي إلي وقوع حوادث كارثية. وكما ذكرنا، فإنه من الممكن أيضًا أن تتعرض المركبة الذكية لبرامج الفدية مما يعني طلب أحد المتطفلين رسومًا مقابل السماح لمالك المركبة بفتحها أو تشغيل محركها.

أجهزة إنترنت الأشياء المزيفة والرديئة:

- أدى الطلب الهائل المتزايد على أجهزة إنترنت الأشياء وحجم الإنتاج إلى ظهور الكثير من الأجهزة المزيفة أو الرديئة، والتي قد تؤدي إلى حدوث مشاكل أمنية عند تثبيتها داخل الشبكات المنزلية الآمنة، في بعض الأحيان يمكن أن تكون هذه الأجهزة نقاط وصول أو كاميرات فيديو أو أجهزة لتنظيم درجة الحرارة وأنواع أخرى من الأجهزة التي تقوم بسرقة البيانات دون علم المستخدم.

ضعف وعي المستخدمين في أمن إنترنت الأشياء:

- يعتبر ضعف الوعي والسلوكيات غير المسؤولة للمستخدمين من أكبر المخاطر التي تهدد أمن استخدام أجهزة إنترنت الأشياء نظرًا لأنه يضع العديد من الأطراف في دائرة الخطر سواء مستخدموا الأجهزة أنفسهم أو من يرتبطون بطريقة أو بأخرى بوحدات إنترنت الأشياء الخاصة بهؤلاء الأشخاص. ومن أبرز تلك السلوكيات، ترك كلمات المرور دون تغيير، أو إهمال تثبيت التحديثات الدورية للأجهزة، مما يترك ثغرات أمنية خطيرة ويفتح المجال للمخترقين والمتلصصين للوصول إلى الأجهزة والتحكم بها.

1

وضح الاختلاف بين الشهادة الرقمية والتوقيع الرقمي.

_____

_____

_____

2

ما المقصود بالتوقيع الرقمي؟ أذكر بعض الأمثلة على استخداماته.

_____

_____

_____

3

قم بفتح **Microsoft Outlook** وقم بتفعيل زر رسالة التوقيع الرقمي. التقط صورة للشاشة لما قمت بعمله.

4

قم بفتح **Microsoft Outlook** وقم بتفعيل زر رسالة التوقيع الرقمي لجميع رسائل البريد الإلكتروني. التقط صورة للشاشة لما قمت بعمله.

5

ما هي شبكة **VPN**؟ أذكر بعض الأمثلة على استخداماتها.

_____

_____

_____

6

اذكر ميزتين وتحديين يواجهان استخدام **VPN**.

_____

_____

_____

7

باستخدام **Microsoft Windows**، أنشئ ملف تشكيل **VPN** جانبي وقم بتوصيله بشبكة **VPN**.

8 اذكر اختلافين بين نظام تشغيل الحواسيب المكتبية ونظام تشغيل أجهزة انترنت الأشياء.

_____

_____

_____

9 عدد بعض مخاطر استخدام أجهزة إنترنت الأشياء.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

10

عدد بعض أجهزة انترنت الأشياء المستخدمة حولنا.

الدرس السادس

التجسس على حزم البيانات Packet Sniffing

التجسس على الحزم هي ممارسة لتجميع وتسجيل حزم البيانات **Packets** التي تمر عبر شبكة الحاسوب، بغض النظر عن طبيعة أو محتوى تلك الحزم. عادة يتم جمع حزم البيانات لأغراض التحليل ومراقبة سرعة نقل البيانات والنطاق الترددي **Bandwidth**.

محلل الحزم

تعد أداة تحليل الحزم (المعروفة أيضًا باسم محلل الحزمة) (**Packet Analyzer**) أحد الأدوات الرئيسة لأي محترف بالأمن الحاسوبي، فهي أداة مهمة تحدد ما إذا كانت عملية نقل المعلومات تتم بأمان. توجد العديد من أدوات التحليل المستخدمة لعمليات نقل البيانات والتي تساعد في التقاط حركة مرور بيانات الشبكة، ومن أكثرها شيوعًا **Wireshark**.

تتطلب عملية تحليل الحزم في الشبكة الأدوات التالية:

أ) بطاقة شبكة تصل محلل الحزم بالشبكة الحالية.

ب) برنامج يوفر طريقة لتسجيل البيانات التي تم جمعها بواسطة الجهاز أو الاطلاع عليها أو تحليلها.

محلل الحزم (**Packet Analyzer**) هو عبارة عن جهاز يقوم باعتراض وتسجيل حركة المرور عبر الشبكة الرقمية أثناء تدفق البيانات، يلتقط هذا المحلل كل حزمة ويقوم بفك تشفير البيانات الأولية للحزمة.

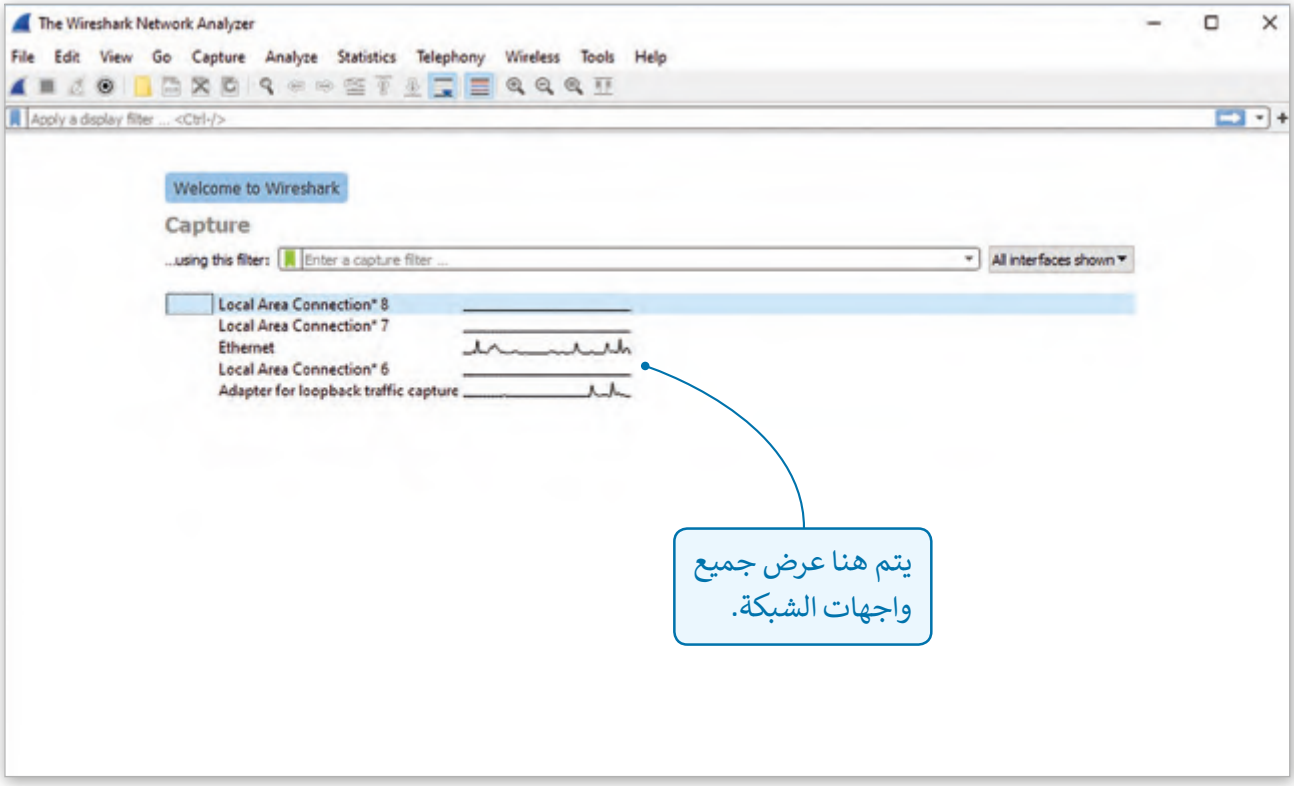
يقوم محلل الحزم بتتبع مشاكل الشبكة، من خلال الوظائف التالية:

- معرفة من يقوم بالتجسس على البيانات عبر الشبكة ومراقبة أنشطة المهاجمين.
- تحديد كيفية عمل ماسحات المنافذ (**port scanners**) وأدوات التحليل الأخرى.
- تحديد البروتوكولات الآمنة والتي تمر عبرها البيانات.
- تحديد العمليات المشبوهة لنقل البيانات.
- التعرف على البرمجيات الضارة واتصالاتها بالخوادم المشبوهة.
- تحديد مصدر البيانات التي تستهلك النصيب الأكبر من موارد الشبكة.

Wireshark

تطبيق **Wireshark** هو أحد التطبيقات مفتوحة المصدر والتي تستخدم في تحليل حزم البيانات، حيث تستخدمه العديد من المؤسسات التجارية وغير الربحية والوكالات الحكومية والمؤسسات التعليمية.

يمكن استخدام **Wireshark** لفحص تفاصيل حركة البيانات على عدة مستويات بدءًا من معلومات مستوى الاتصال إلى مستوى معلومات الحزمة الواحدة، بحيث يوفر المعلومات لمسؤول الشبكة بخصوص الحزم الفردية مثل وقت الإرسال والمصدر والوجهة ونوع البروتوكول وبيانات رأس الحزمة **Header** وهي بيانات قد تكون مهمة جدًا لتقييم وتشخيص مشكلات أمن الشبكة.



تشغيل برنامج Wireshark

لنجرب تشغيل برنامج **Wireshark** ونلاحظ طريقة مسح البيانات المتدفقة عبر الشبكة.

لالتقاط الحزم:

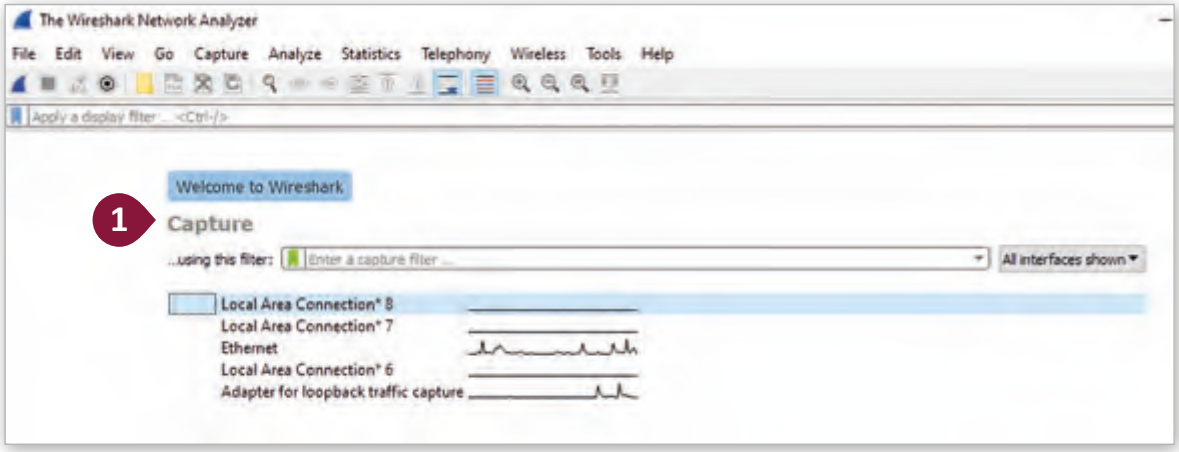
> افتح برنامج **Wireshark** واضغط ضغطًا مزدوجًا فوق **Capture** (التقاط). ❶

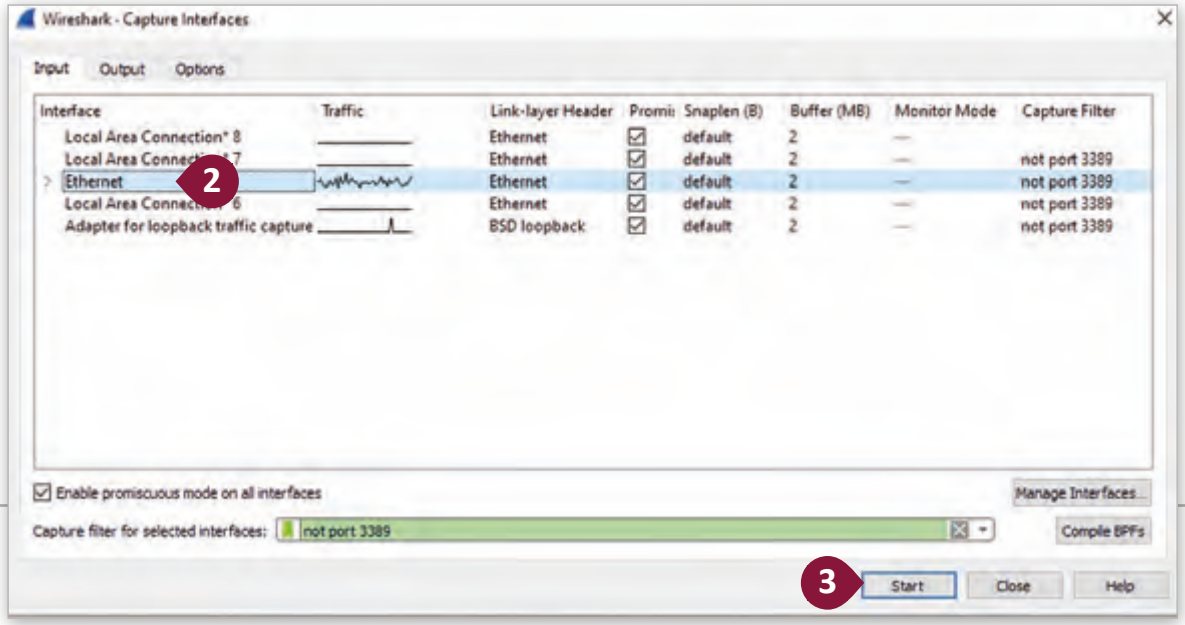
> من قائمة واجهة الشبكة التي تظهر، اختر واجهة الاتصال **Interface** التي تريد مراقبتها. ❷

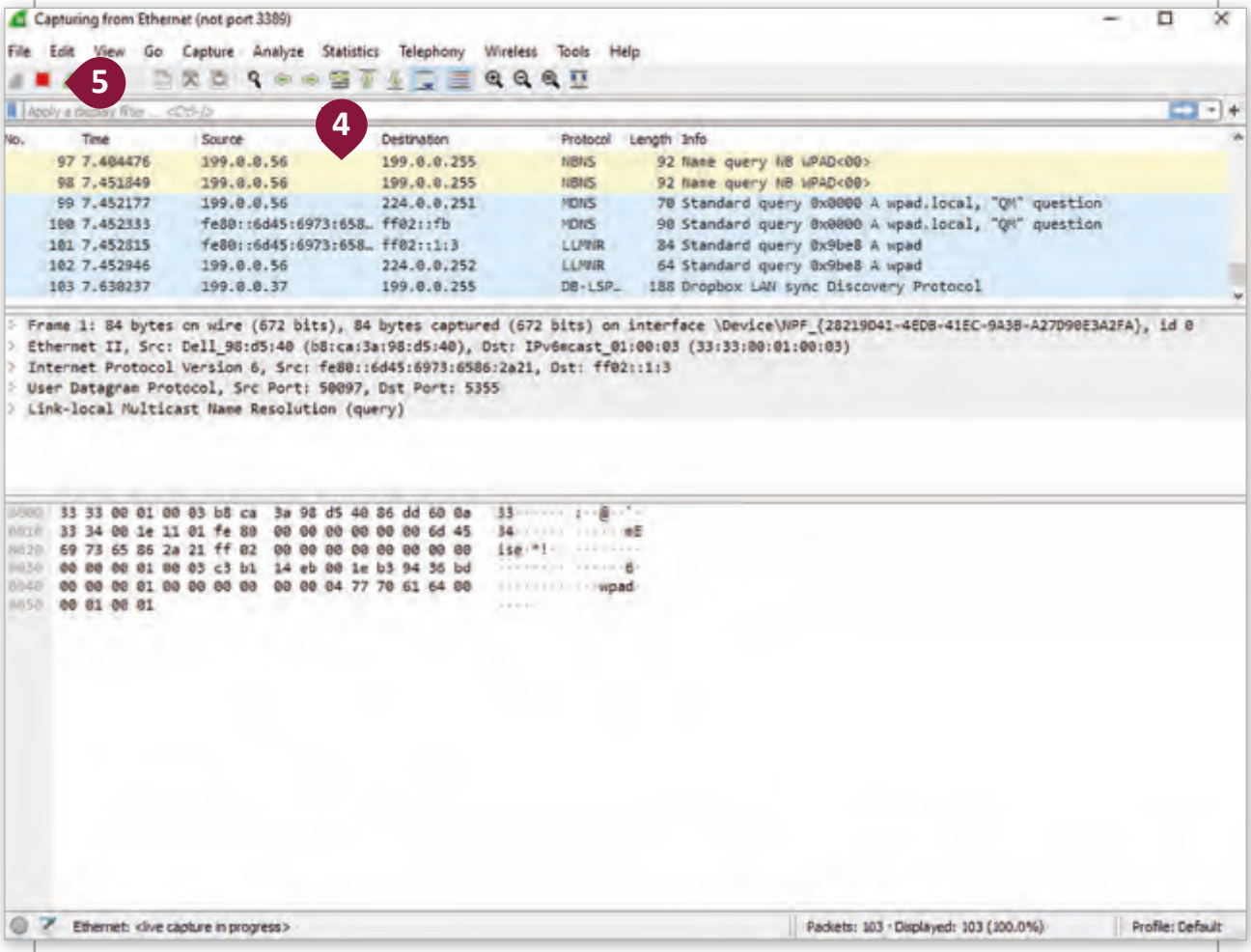
> اضغط فوق **Start** (ابدأ). ❸

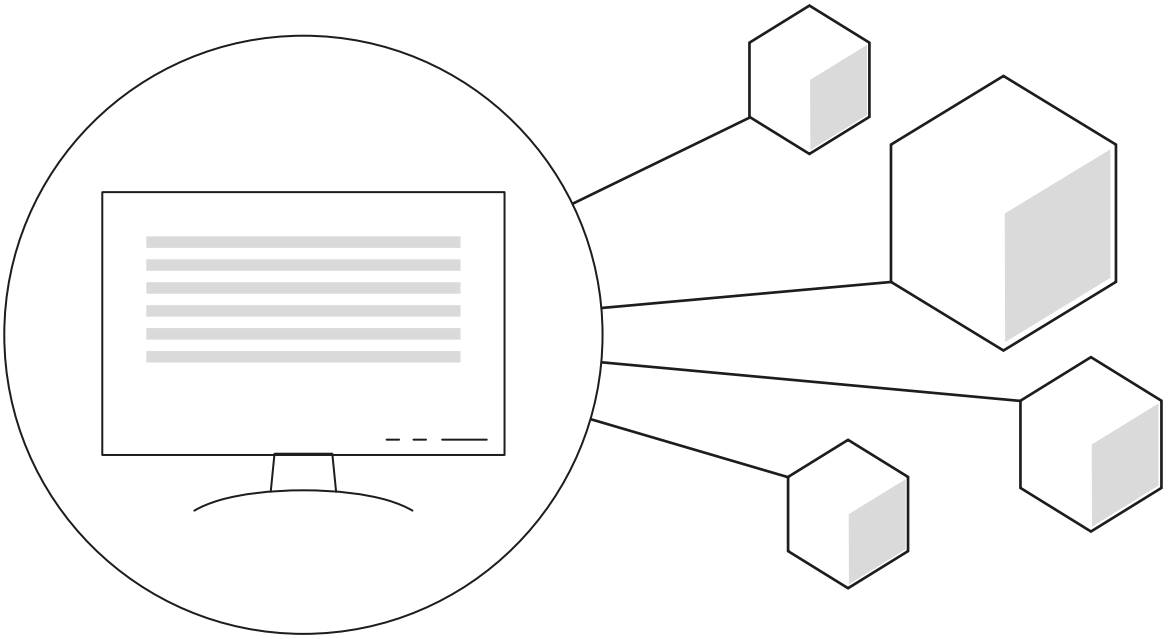
> لاحظ تدفق حزم البيانات التي يظهرها البرنامج. ❹

> اضغط فوق **Stop** (إيقاف). ❺





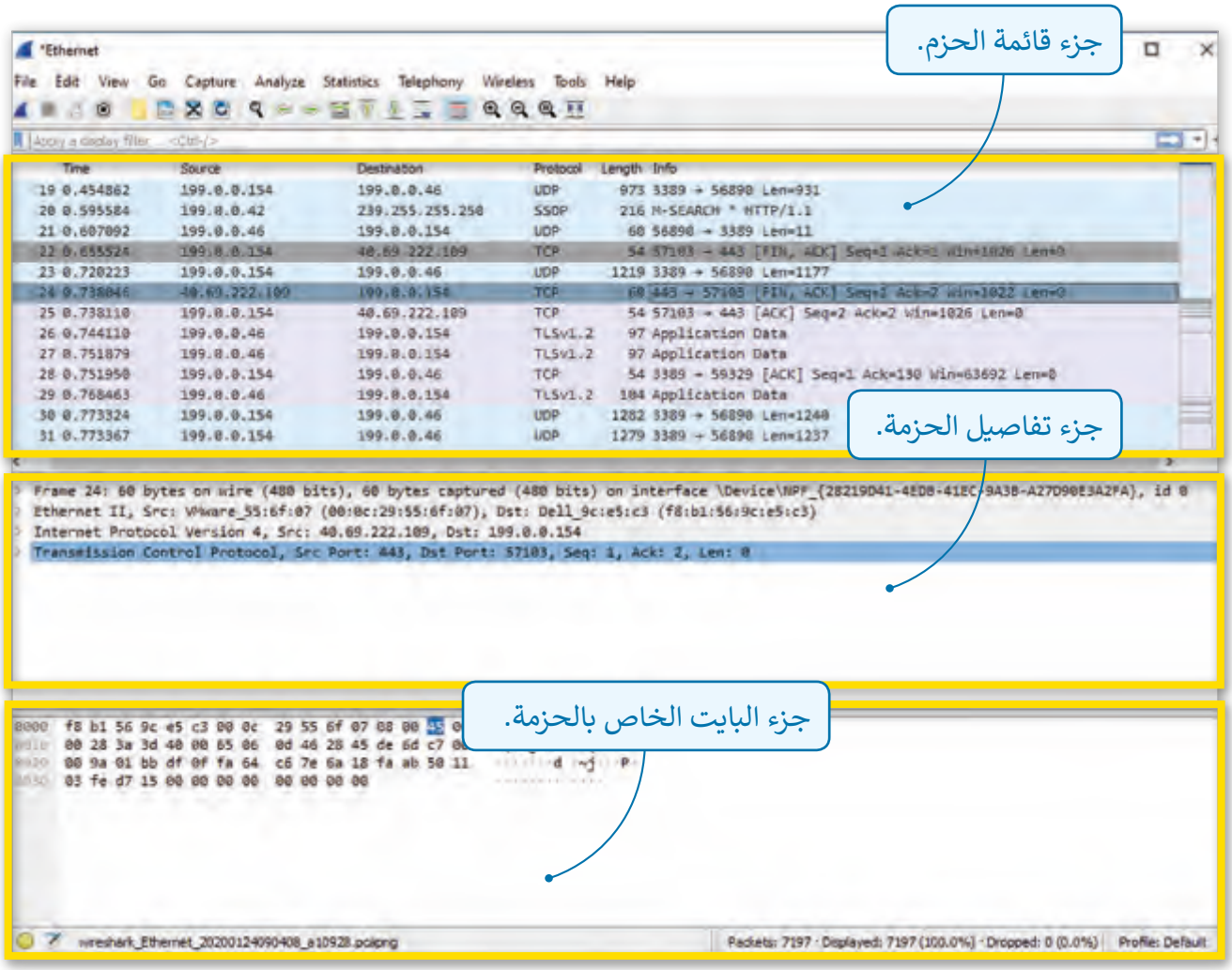

Capturing from Ethernet (not port 3389)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
5
4
No. Time Source Destination Protocol Length Info
97 7.404476 199.0.0.56 199.0.0.255 NBNS 92 Name query NB WPAD<00>
98 7.451849 199.0.0.56 199.0.0.255 NBNS 92 Name query NB WPAD<00>
99 7.452177 199.0.0.56 224.0.0.251 MDNS 70 Standard query 0x0000 A wpad.local, "QM" question
100 7.452333 fe80::6d45:6973:658… ff02::fb MDNS 90 Standard query 0x0000 A wpad.local, "QM" question
101 7.452815 fe80::6d45:6973:658… ff02::1:3 LLMNR 84 Standard query 0x9be8 A wpad
102 7.452946 199.0.0.56 224.0.0.252 LLMNR 64 Standard query 0x9be8 A wpad
103 7.638237 199.0.0.37 199.0.0.255 DB-LSP… 188 Dropbox LAN sync Discovery Protocol
Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{28219D41-4ED8-41EC-9A3B-A27D90E3A2FA}, id 0
Ethernet II, Src: Dell_98:d5:40 (b8:ca:3a:98:d5:40), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
Internet Protocol Version 6, Src: fe80::6d45:6973:6586:2a21, Dst: ff02::1:3
User Datagram Protocol, Src Port: 50097, Dst Port: 5355
Link-local Multicast Name Resolution (query)
33 33 00 01 00 03 b8 ca 3a 98 d5 40 86 dd 60 0a
33 34 00 1e 11 01 fe 80 00 00 00 00 00 00 6d 45
69 73 65 86 2a 21 ff 02 00 00 00 00 00 00 00 00
00 00 00 01 00 03 c3 b1 14 eb 00 1e b3 94 36 bd
00 00 00 01 00 00 00 00 00 00 04 77 70 61 64 00
00 01 00 01
Ethernet: <live capture in progress>
Packets: 103 · Displayed: 103 (100.0%)
Profile: Default



ما نوع المعلومات التي نستقبلها؟

توفر واجهة مستخدم **Wireshark** ثلاثة أجزاء رئيسة كالتالي:

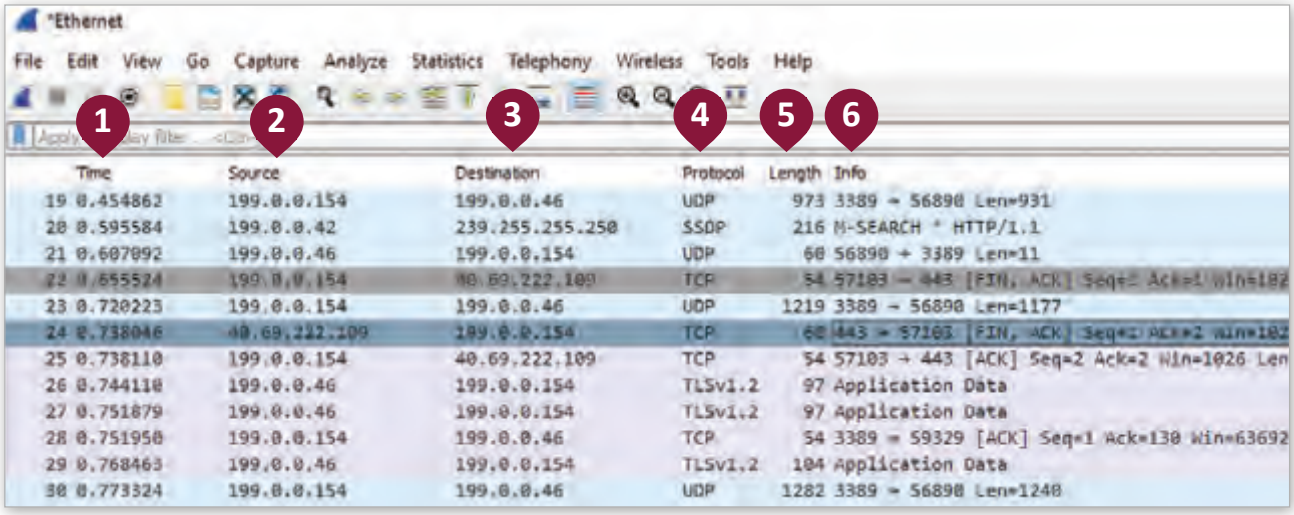
1. جزء قائمة الحزم (**Packet List Pane**).
2. جزء تفاصيل الحزمة (**Packet Details Pane**).
3. جزء البايت الخاص بالحزمة (**Packet Byte Pane**).

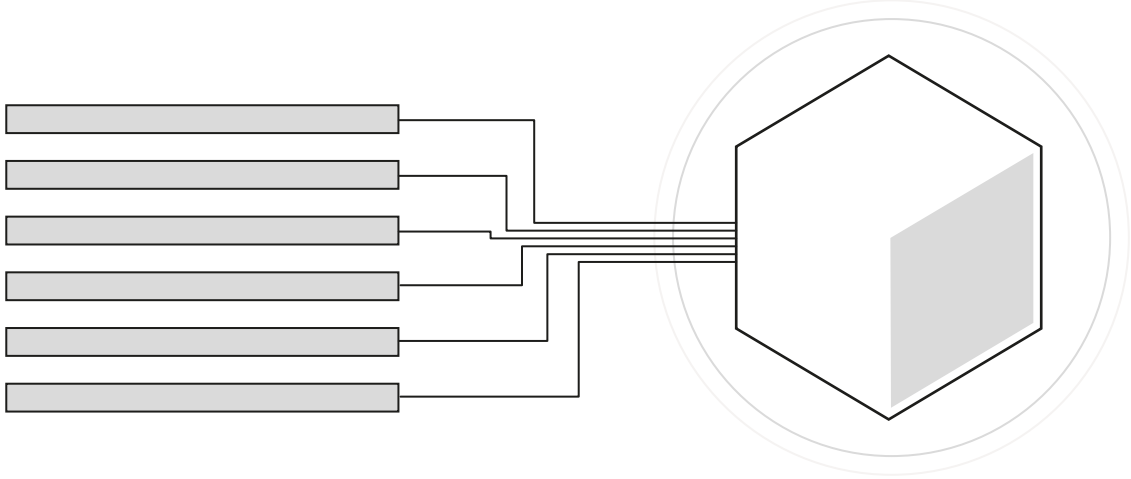


جزء قائمة الحزم (Packet List Pane)

يعرض هذا الجزء قائمة بجميع الحزم التي يتم التقاطها، وتشمل المعلومات التي نتلقاها في **Wireshark** كل من:

1. **Time** (الوقت): ويشير إلى الوقت الذي تم فيه استلام الحزمة أو إرسالها، وبالتحديد يشير إلى الثواني منذ بداية الالتقاط.
2. **Source** (المصدر): يشير إلى عنوان **IP** للمصدر.
3. **Destination** (الوجهة): تشير إلى عنوان **IP** الخاص بالوجهة.
4. **Protocol** (البروتوكول): يشير إلى البروتوكول الذي تم استخدامه.
5. **Length** (الطول): يشير إلى طول الحزمة.
6. **Info** (المعلومات): يحتوي معلومات إضافية حول الحزمة.

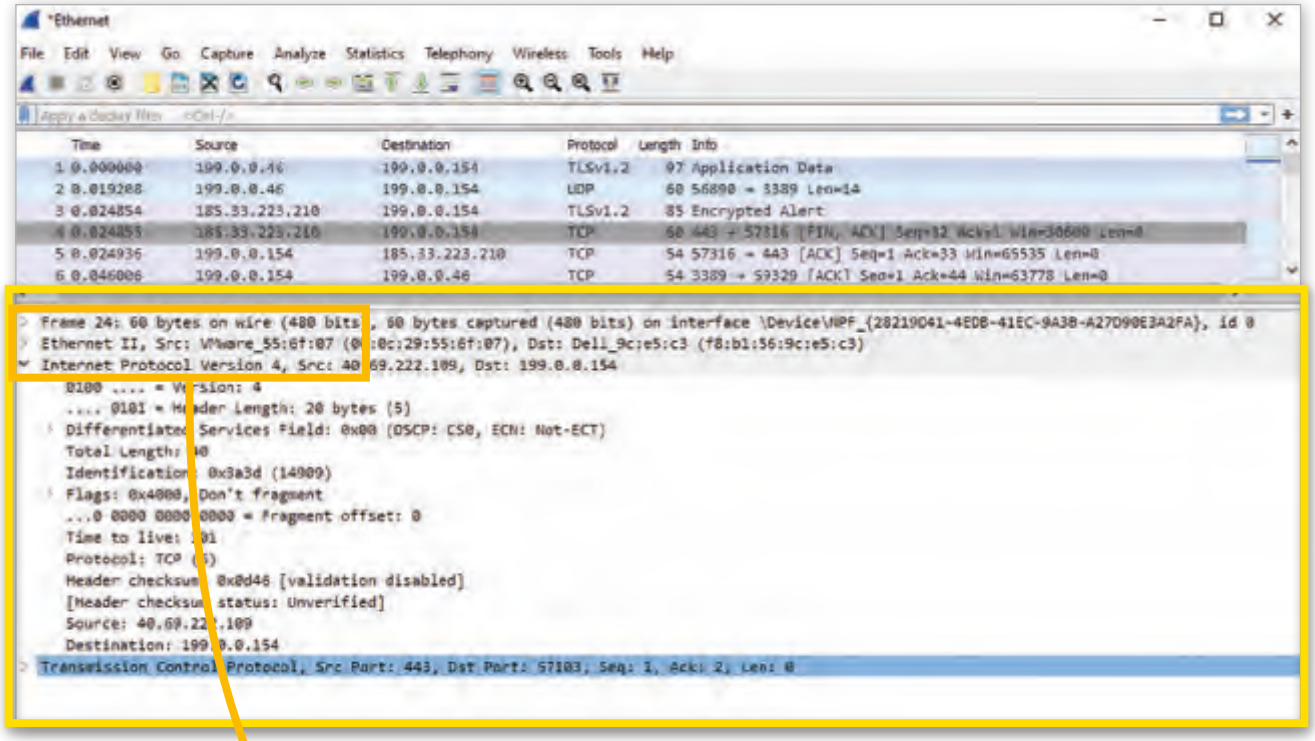


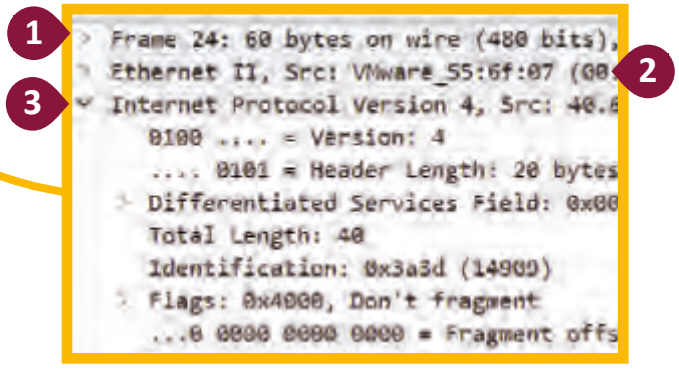


جزء تفاصيل الحزمة (Packet Details Pane)

يصف هذا الجزء حزمة محددة بشكل موسع، فيمكننا الضغط فوق الأسهم المنسدلة لعرض المزيد من المعلومات حول:

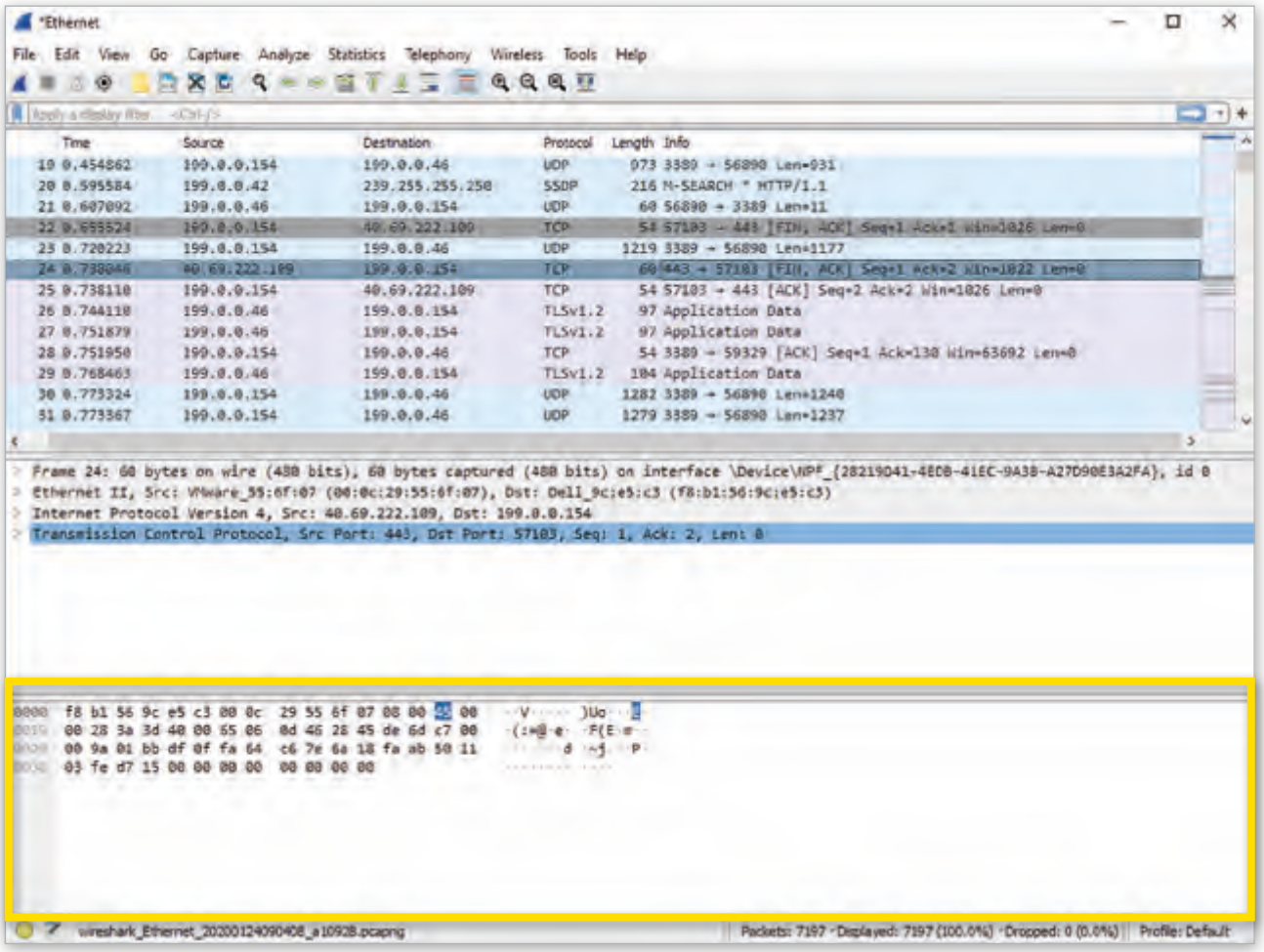
1. الإطار (**Frame**).
2. الإيثرنت (**Ethernet**).
3. بروتوكول الإنترنت (**IP**).

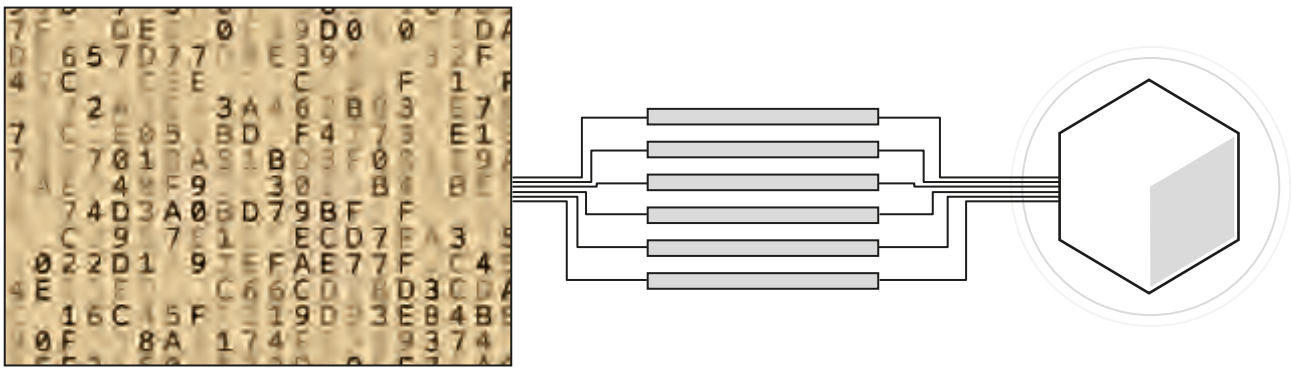




جزء البايت الخاص بالحزمة (Packet Byte Pane)

يعرض هذا الجزء بيانات حزمة محددة بالتنسيق الستة عشري **Hexadecimal** الخاص ببيانات الحاسوب.





فتح نتائج مسح ملف Wireshark

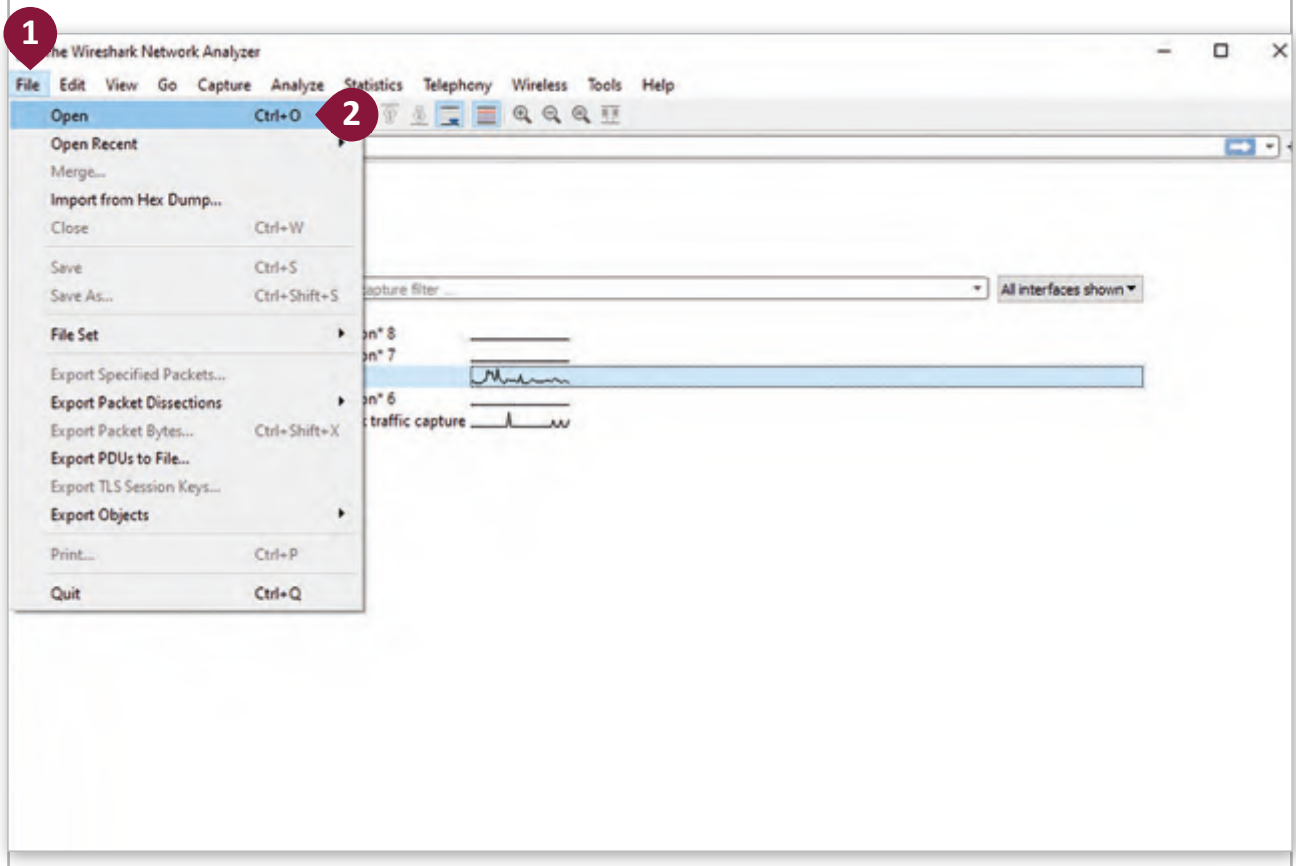
يمكن حفظ ملفات مسح **Wireshark** من أجل فتحها في أي وقت لمزيد من الفحص والتدقيق. دعنا نفتح ملف **Wireshark** موجود لمعرفة نوع البيانات التي يمكن أن نستخلصها منه.

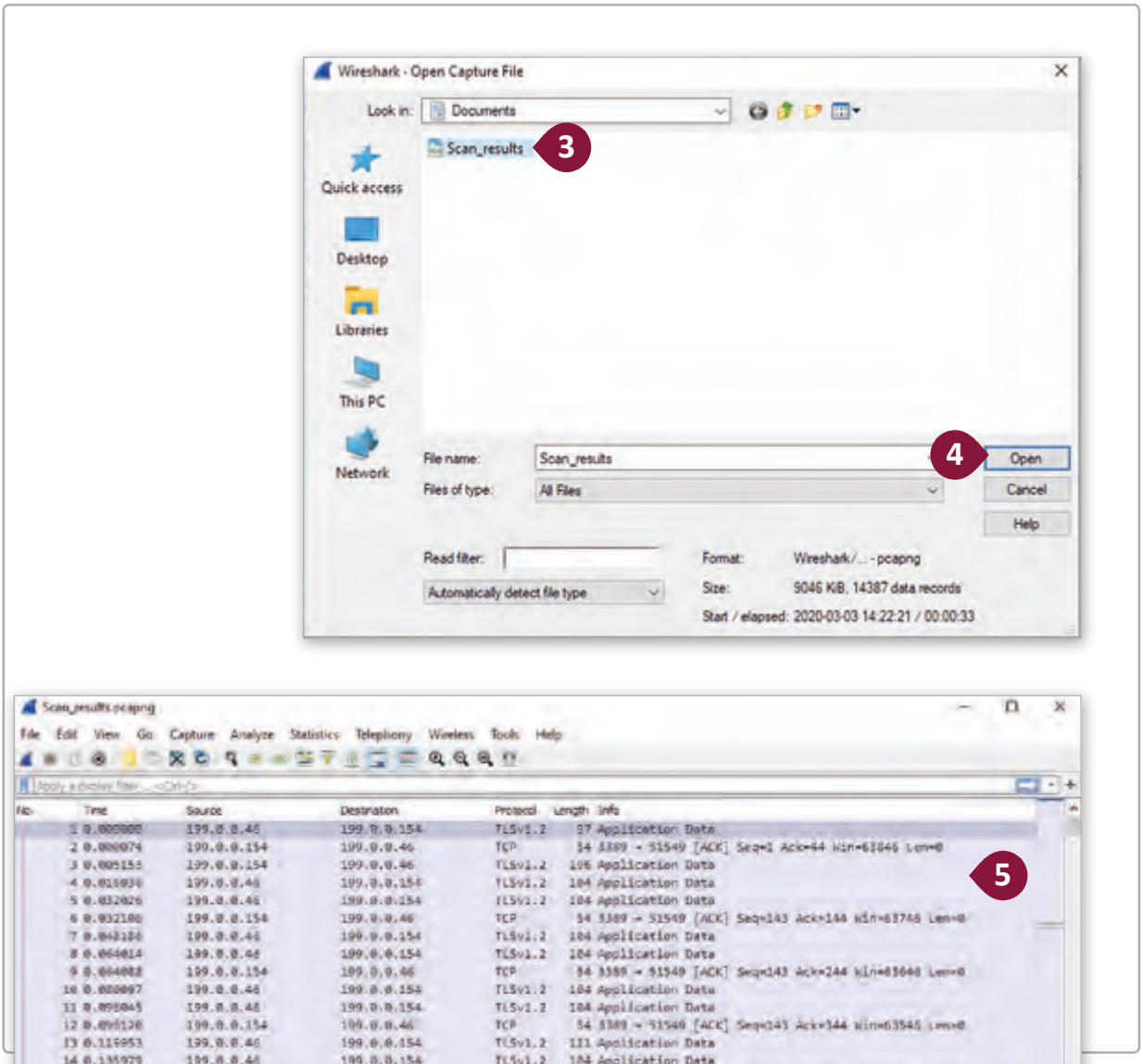
لفتح ملف Wireshark:

> في علامة التبويب **File** (ملف)، ❶ اضغط فوق **Open** (فتح). ❷

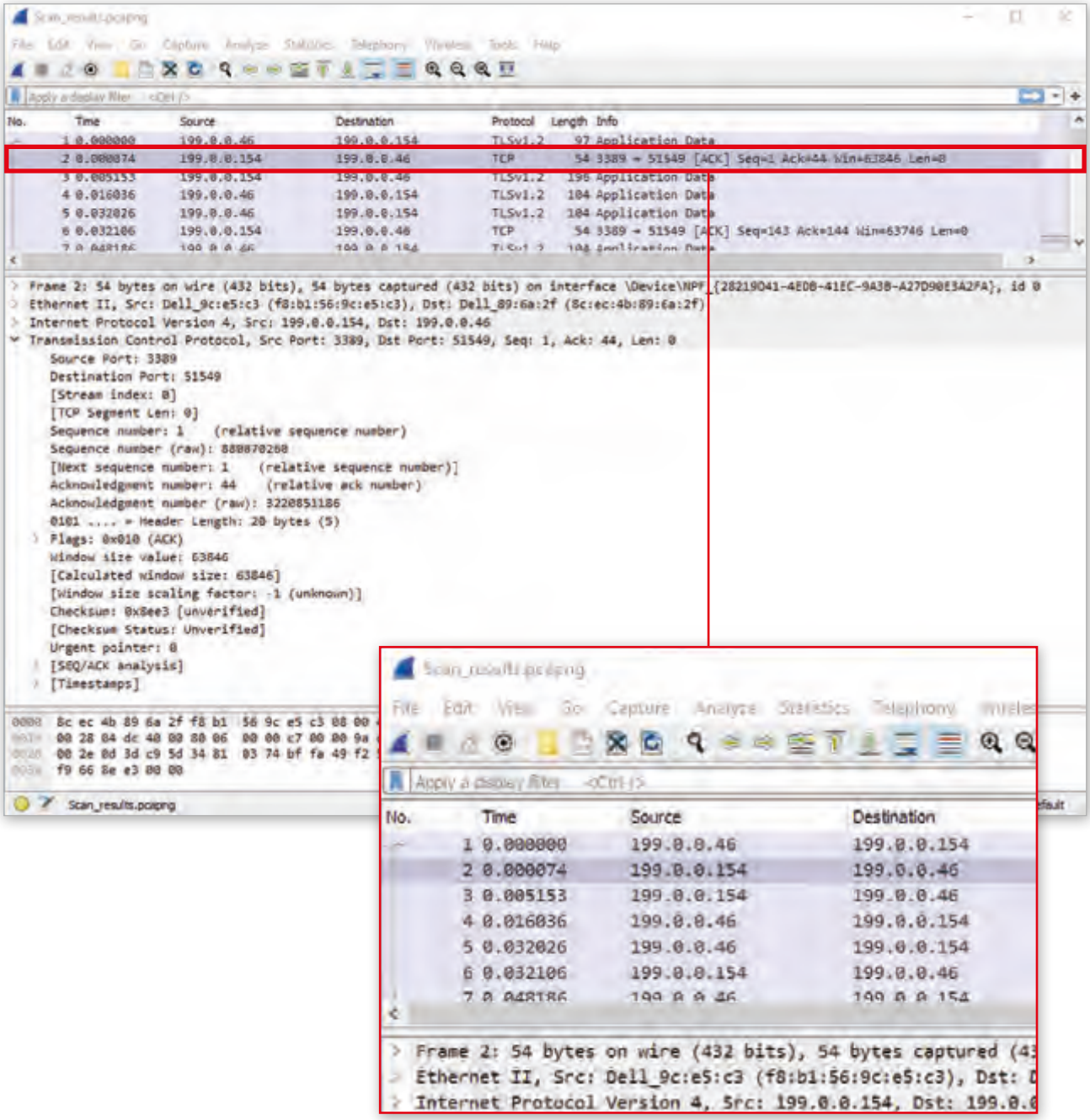
> في نافذة **Open Capture File**، اختر الملف ❸ واضغط فوق **Open** (فتح). ❹

> سيظهر ملف المسح. ❺

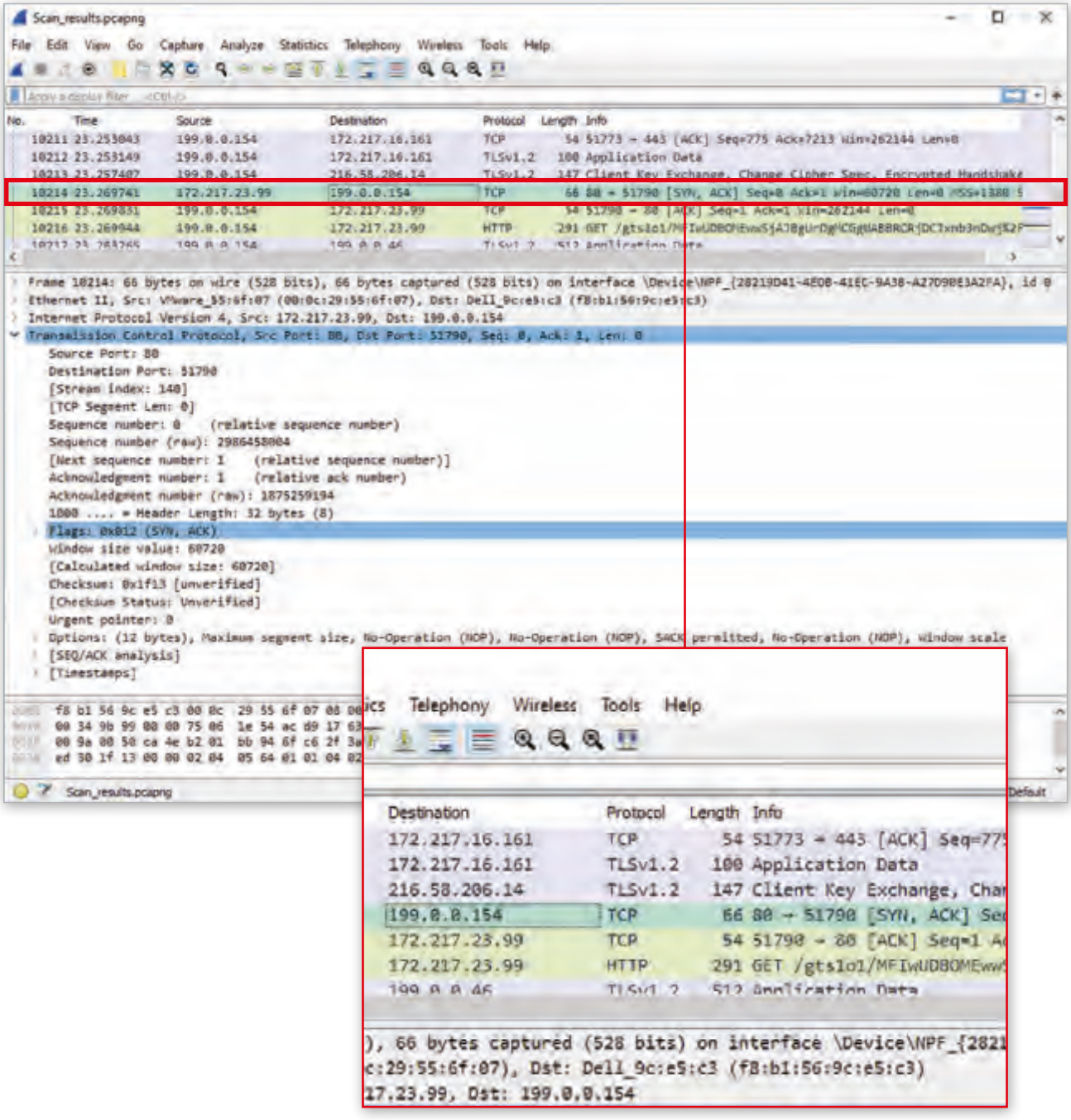



Wireshark - Open Capture File
Look in: Documents
Scan_results
3
Quick access
Desktop
Libraries
This PC
Network
File name: Scan_results
4
Open
Files of type: All Files
Cancel
Help
Read filter:
Format: Wireshark/... - pcapng
Automatically detect file type
Size: 9046 KiB, 14387 data records
Start / elapsed: 2020-03-03 14:22:21 / 00:00:33
Scan_results.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
5
Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{28219D41-4ED8-41EC-9A3B-A27C90E3A2FA}, id 0
Ethernet II, Src: Dell_89:6a:2f (8c:ec:4b:89:6a:2f), Dst: Dell_9c:e5:c3 (f8:b1:56:9c:e5:c3)
Internet Protocol Version 4, Src: 199.0.0.46, Dst: 199.0.0.154
Transmission Control Protocol, Src Port: 51549, Dst Port: 3389, Seq: 1, Ack: 1, Len: 43
Transport Layer Security
Packets: 14387 · Displayed: 14387 (100.0%)
Profile: Default

من خلال إلقاء نظرة فاحصة على **Packet List Pane** (جزء قائمة الحزم) الذي يعرض نتائج المسح، يمكننا أن نلاحظ أن ملف المسح يحتوي على حزم تصف المحادثات بين أجهزة المستخدمين (الأجهزة العميلة) والخوادم المركزية. وبشكل أكثر تحديدًا، في الحزمة رقم 2، يمكننا ملاحظة أن عنوان **IP** للمتلقي هو 199.0.0.154 وأن عنوان **IP** للمرسل هو 199.0.0.46. يرسل المتلقي حزمة باستخدام بروتوكول **TCP** للمرسل، عبر المنفذ 3389 كمنفذ مصدر (منفذ المتلقي) والمنفذ 51549 كمنفذ وجهة (منفذ المرسل).



الآن، دعونا نلقي نظرة على مثال حزمة أخرى. في الحزمة رقم 10214 يمكننا أن نلاحظ أن عنوان **IP** للمرسل هو 172.217.23.99 وأن عنوان **IP** للمستقبل هو 199.0.0.154. كما تظهر معلومات الحزمة أن بروتوكول الإرسال المستخدم هو بروتوكول **TCP**، وأن رقم المنفذ هو 80، ويشير ذلك إلى استخدام بروتوكول نقل النص التشعبي (**HTTP**). وهذا يعني أن المستخدم (الوجهة) يزور صفحة ويب. بشكل أكثر تحديدًا، ينتمي **IP** 172.217.23.99 إلى صفحة محرك بحث **Google** وهذا يعني أن **Google** قد أرسلت لنا حزمة.



كشف النشاط المشبوه بواسطة Wireshark

يتم استخدام **Wireshark** لاكتشاف الأنشطة المشبوهة في شبكتنا، وبالتحديد سنتحقق من بروتوكولات **ARP** والحزم التي تمر باستخدام هذا البروتوكول لاكتشاف الأجهزة التي تحاول القيام بأي عمليات مشبوهة.

للكشف عن طلبات ARP:

> من علامة تبويب **Edit** (تحرير)، ❶, اضغط فوق **Preferences** (التفضيلات). ❷

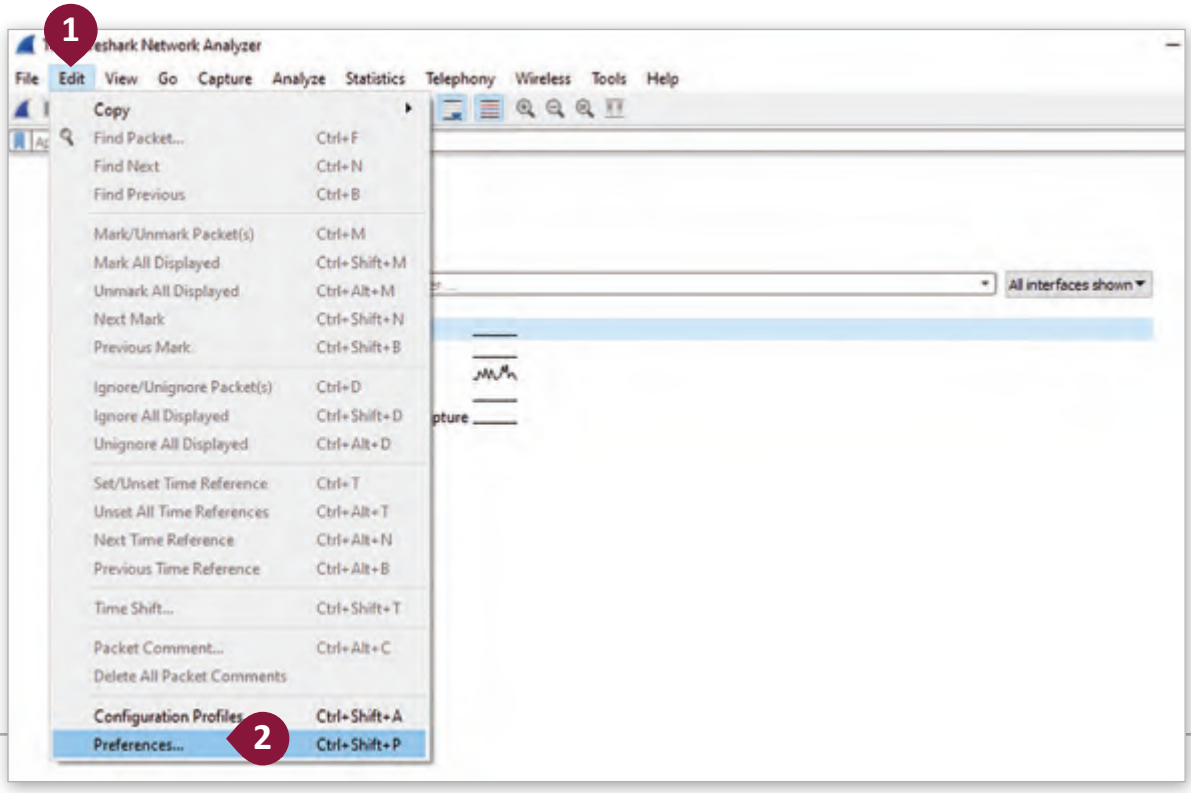
> في نافذة التفضيلات، حدد **Protocols** (البروتوكولات). ❸

> اختر بروتوكول **ARP/RARP**. ❹

> حدد صندوق **Detect ARP request storms** (الكشف عن طلبات **ARP**). ❺

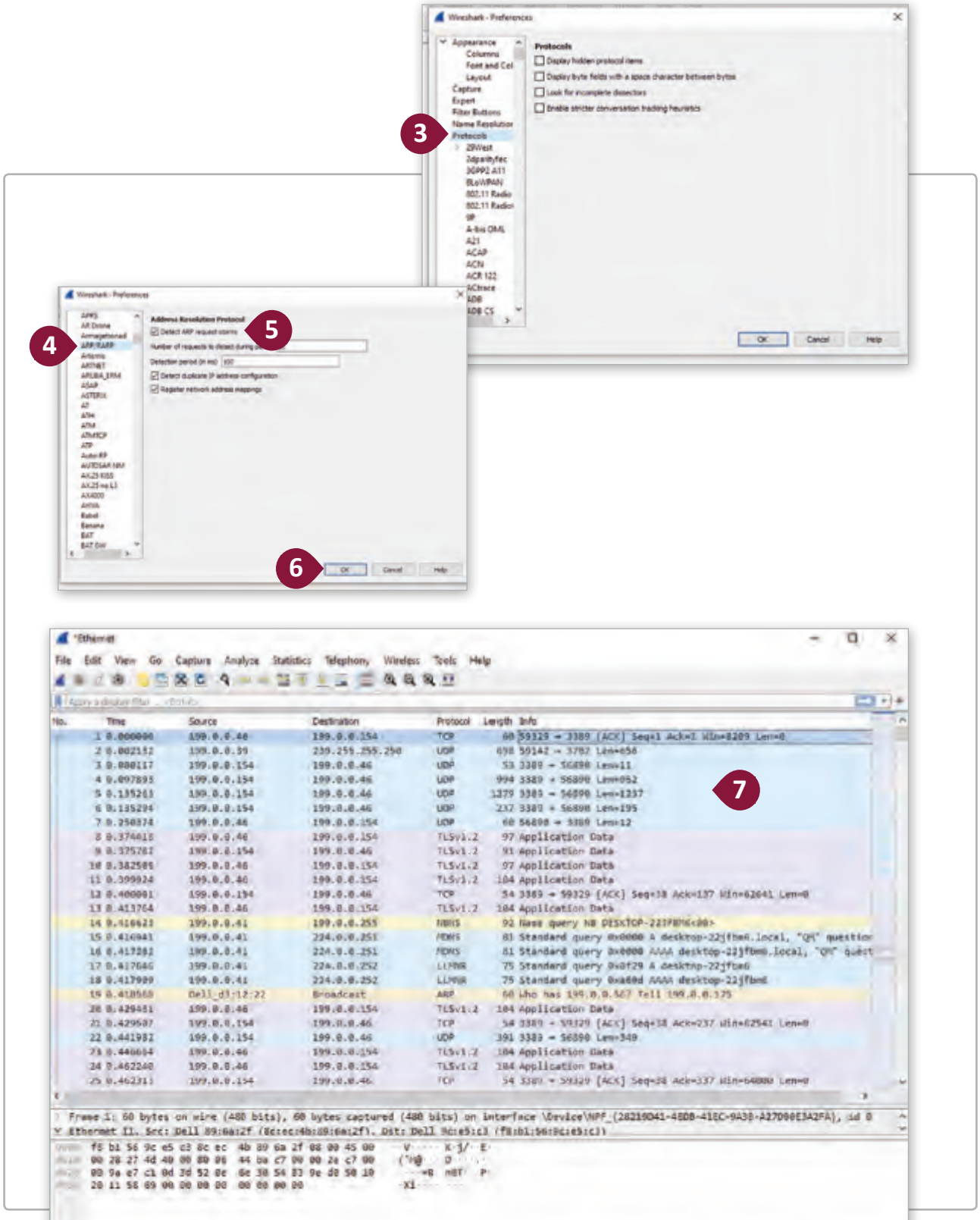
> اضغط **OK** (تم). ❻

> في جزء قائمة الحزم، يمكننا التحقق من وجود نشاط مشبوه. ❼

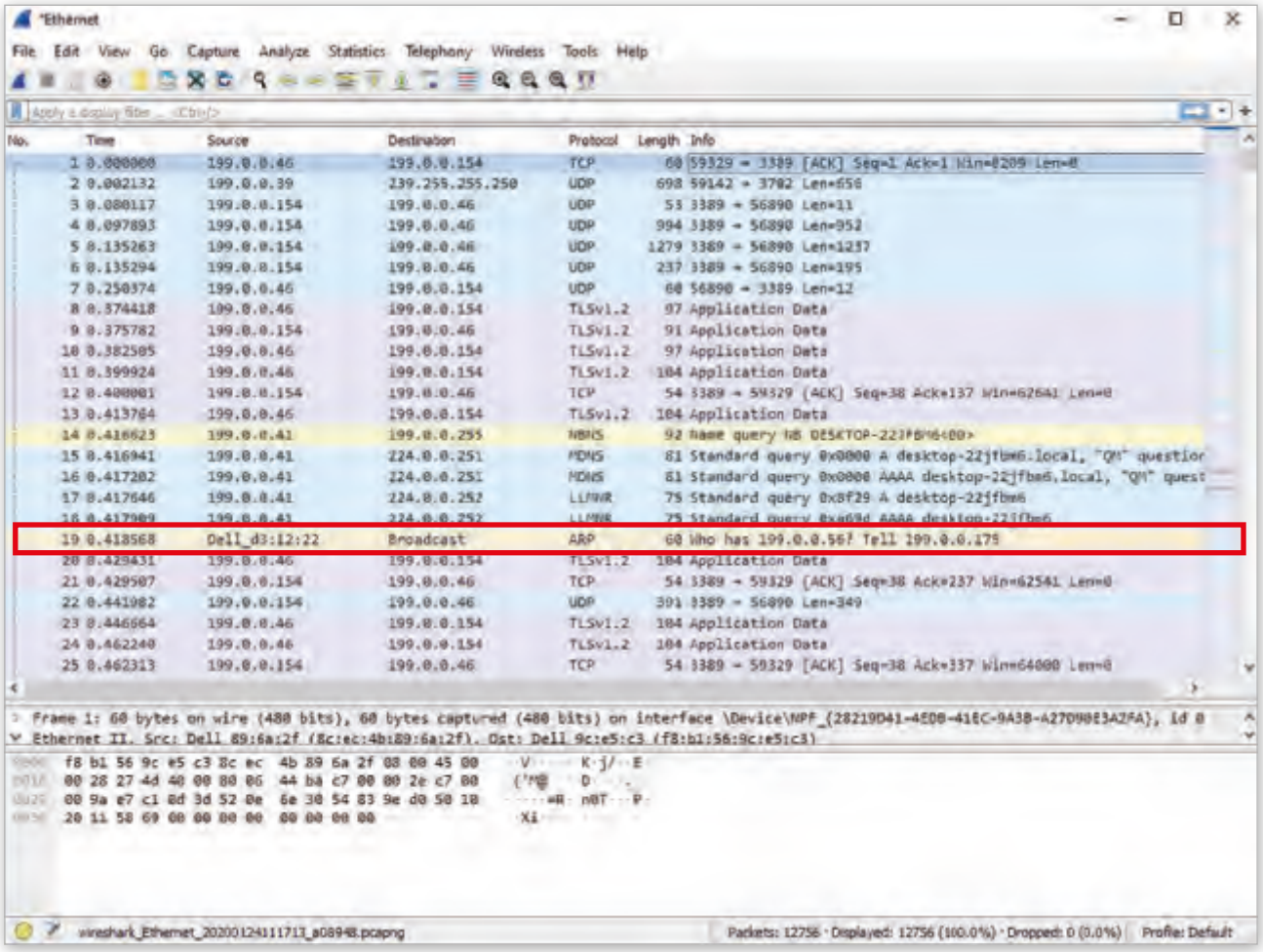


نصيحة ذكية

بروتوكول تحليل العنوان (ARP) هو بروتوكول اتصال يستخدم لاكتشاف العنوان الفعلي المرتبط بعنوان شبكة معين، في حين أن Reserve ARP (RARP) هو بروتوكول شبكة يستخدمه جهاز عميل في شبكة محلية لطلب عنوان بروتوكول الإنترنت الخاص به (IPv4) من جدول ARP لبوابة الموجه.


3
4
5
6
7

من خلال إلقاء نظرة فاحصة على جزء قائمة الحزم الذي يعرض نتائج الالتقاط لشبكة الإيثرنت يمكننا أن نلاحظ أنه قد تم رصد نشاط مشبوه.



بالتحديد هناك جهاز (مصدر) يُرسل بيانات دون ظهور الوجهة التي يرسل إليها، كما أنه يتلصص على أجهزة أخرى على الشبكة، فالجهاز بعنوان **IP** 199.0.0.175 يتساءل عن الجهاز بعنوان **IP** 199.0.0.56.

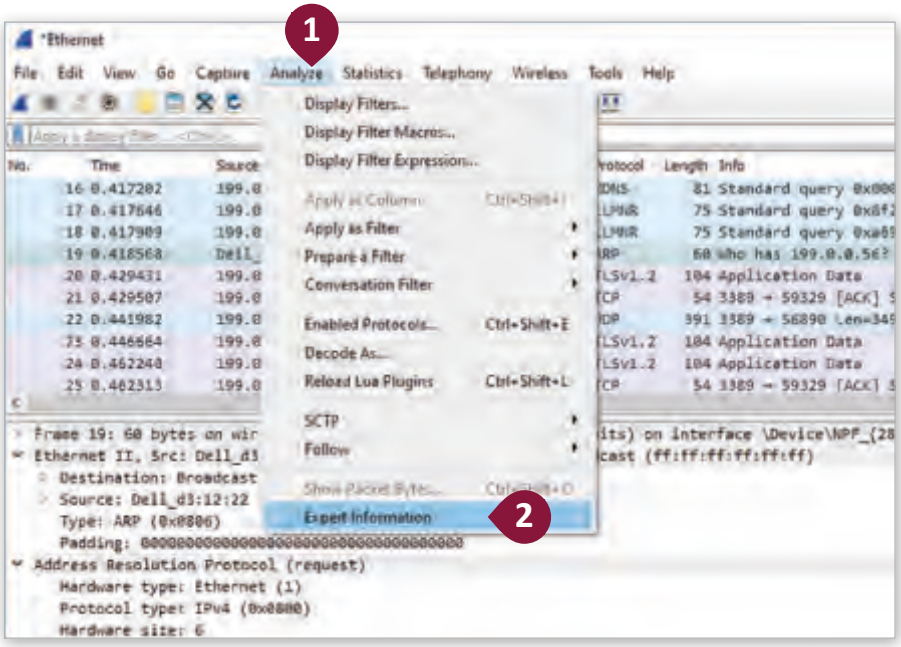
يتم التحقق مما إذا كان **IP** 199.0.0.56 قيد الاستخدام ويتم إرجاع الاستجابة إلى **IP** 199.0.0.175 ، ومن خلال هذه المعلومات يمكننا أن نستنتج أنه ربما يحاول شخص ما اكتشاف ما إذا كان **IP** 199.0.0.56 قيد الاستخدام، فإذا لم يكن كذلك، سيتمكن المتسلل (المخترق) من استخدام عنوان **IP** هذا للاتصال بالشبكة.

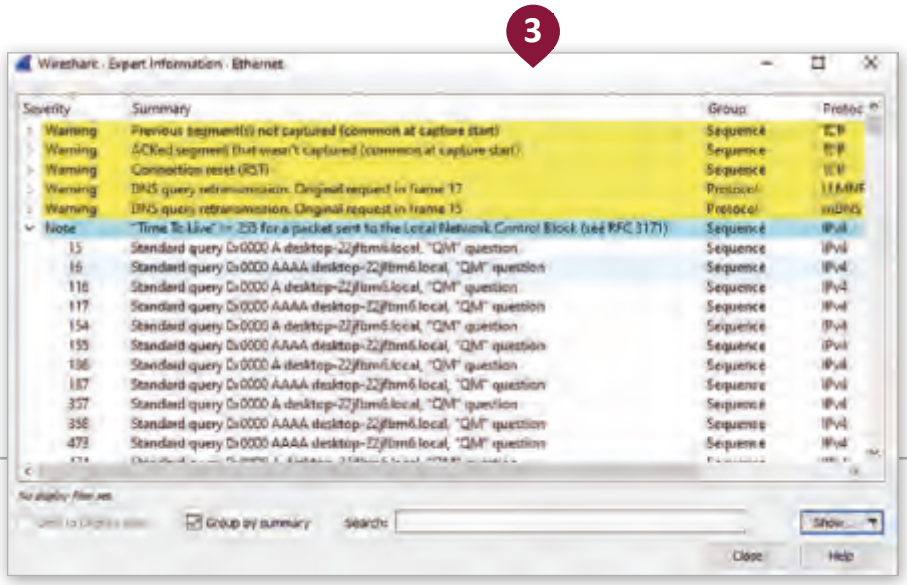
يقدم برنامج **Wireshark** خيار "معلومات الخبير" **Expert Information** لحصر مشاكل الشبكة والسلوكيات المشبوهة عليها، وهو يسهل عملية رصد مثل هذه الأنشطة لغير المحترفين.

لعرض معلومات الخبير:

> من علامة تبويب **Analyze** (تحليل)، ❶ اضغط **Expert Information** (معلومات الخبير). ❷

> ستظهر نافذة معلومات الخبير. ❸

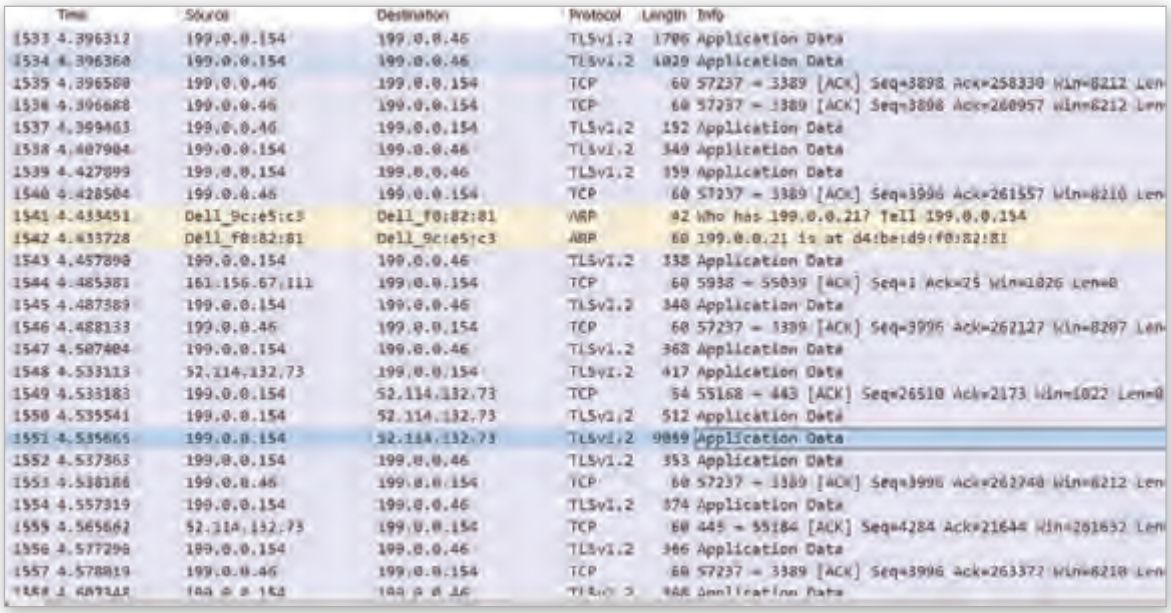




من خلال إلقاء نظرة فاحصة على نافذة معلومات الخبير، يمكننا ملاحظة ما إذا كان قد تم اكتشاف مجموعة حزمة **ARP**، وفي حالتنا هذه تم اكتشاف الأنشطة الاعتيادية للشبكة فقط، لذلك يمكننا استنتاج أن شبكتنا آمنة.

1

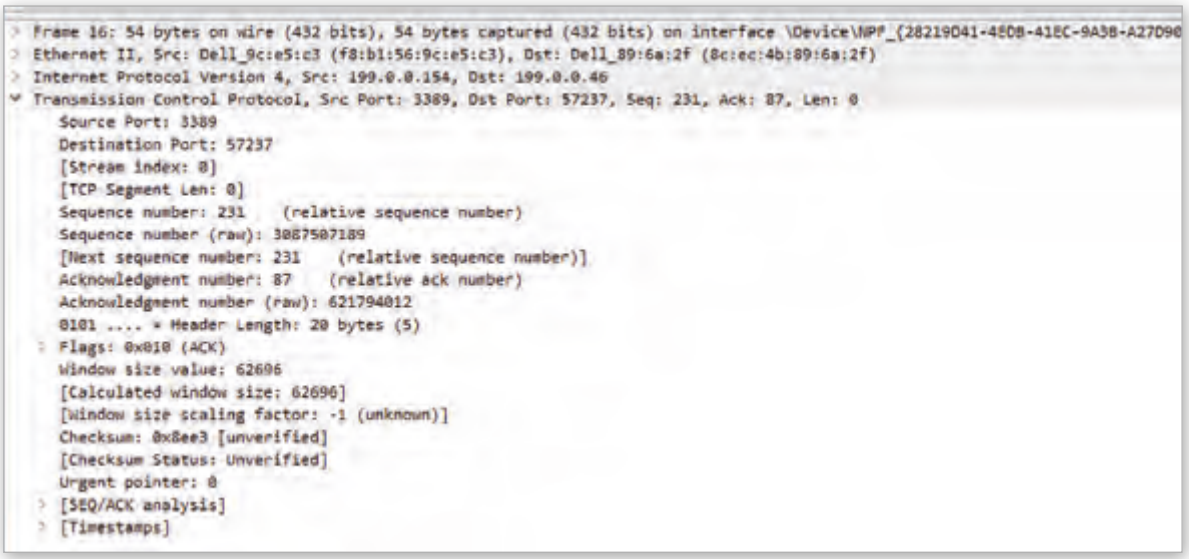
صف نوع المعلومات التي يمكننا استخراجها من ملف المسح التالي باستخدام البيانات المعروضة في قائمة الحزم.



Time	Source	Destination	Protocol	Length	Info
1533 4.396312	199.0.0.154	199.0.0.46	TLSv1.2	1706	Application Data
1534 4.396360	199.0.0.154	199.0.0.46	TLSv1.2	4039	Application Data
1535 4.396580	199.0.0.46	199.0.0.154	TCP	60	57237 → 3389 [ACK] Seq=3898 Ack=258330 Win=8212 Len
1536 4.396688	199.0.0.46	199.0.0.154	TCP	60	57237 → 3389 [ACK] Seq=3898 Ack=260957 Win=8212 Len
1537 4.399463	199.0.0.46	199.0.0.154	TLSv1.2	192	Application Data
1538 4.407904	199.0.0.154	199.0.0.46	TLSv1.2	340	Application Data
1539 4.427899	199.0.0.154	199.0.0.46	TLSv1.2	159	Application Data
1540 4.428504	199.0.0.46	199.0.0.154	TCP	60	57237 → 3389 [ACK] Seq=3996 Ack=261557 Win=8210 Len
1541 4.433451	Dell_9c:e5:c3	Dell_f0:82:81	ARP	42	Who has 199.0.0.21? Tell 199.0.0.154
1542 4.433728	Dell_f0:82:81	Dell_9c:e5:c3	ARP	60	199.0.0.21 is at d4:be:d9:f0:82:81
1543 4.457898	199.0.0.154	199.0.0.46	TLSv1.2	338	Application Data
1544 4.485381	161.156.67.111	199.0.0.154	TCP	60	5938 → 55039 [ACK] Seq=1 Ack=75 Win=1026 Len=0
1545 4.487389	199.0.0.154	199.0.0.46	TLSv1.2	340	Application Data
1546 4.488133	199.0.0.46	199.0.0.154	TCP	60	57237 → 3389 [ACK] Seq=3996 Ack=262127 Win=8207 Len
1547 4.507404	199.0.0.154	199.0.0.46	TLSv1.2	368	Application Data
1548 4.533113	52.114.132.73	199.0.0.154	TLSv1.2	417	Application Data
1549 4.533183	199.0.0.154	52.114.132.73	TCP	54	55168 → 443 [ACK] Seq=26510 Ack=2173 Win=1022 Len=0
1550 4.535541	199.0.0.154	52.114.132.73	TLSv1.2	512	Application Data
1551 4.535665	199.0.0.154	52.114.132.73	TLSv1.2	9069	Application Data
1552 4.537363	199.0.0.154	199.0.0.46	TLSv1.2	353	Application Data
1553 4.538186	199.0.0.46	199.0.0.154	TCP	60	57237 → 3389 [ACK] Seq=3996 Ack=262740 Win=8212 Len
1554 4.557319	199.0.0.154	199.0.0.46	TLSv1.2	374	Application Data
1555 4.565662	52.114.132.73	199.0.0.154	TCP	60	443 → 55184 [ACK] Seq=4284 Ack=21644 Win=261632 Len
1556 4.577298	199.0.0.154	199.0.0.46	TLSv1.2	386	Application Data
1557 4.578819	199.0.0.46	199.0.0.154	TCP	60	57237 → 3389 [ACK] Seq=3996 Ack=263372 Win=8210 Len

2

صف نوع المعلومات التي يمكننا استخراجها من ملف المسح التالي باستخدام البيانات الواردة في جزء تفاصيل الحزمة.



3

ما المقصود بالتجسس على الحزم؟ وماهي الأدوات التي تتطلبها عملية تحليل الحزم؟

4

اذكر الوظائف التي يقوم بها محلل الحزم لتتبع مشاكل الشبكة.

مشروع الوحدة

العنوان: يوم حماية البيانات / يوم خصوصية البيانات (28 يناير)

الوصف: بمناسبة يوم حماية البيانات، عليك أن تستخدم **Microsoft Word** وتنشئ قائمة تحقق تساعد الأشخاص في إدارة سمعتهم والمحافظة عليها عبر الإنترنت.

الأدوات: **Microsoft Edge, Google search engine, Microsoft Word, Microsoft Outlook.**

خطوات التنفيذ:

افتح **Microsoft Edge**.

قم بزيارة **https://www.google.com**

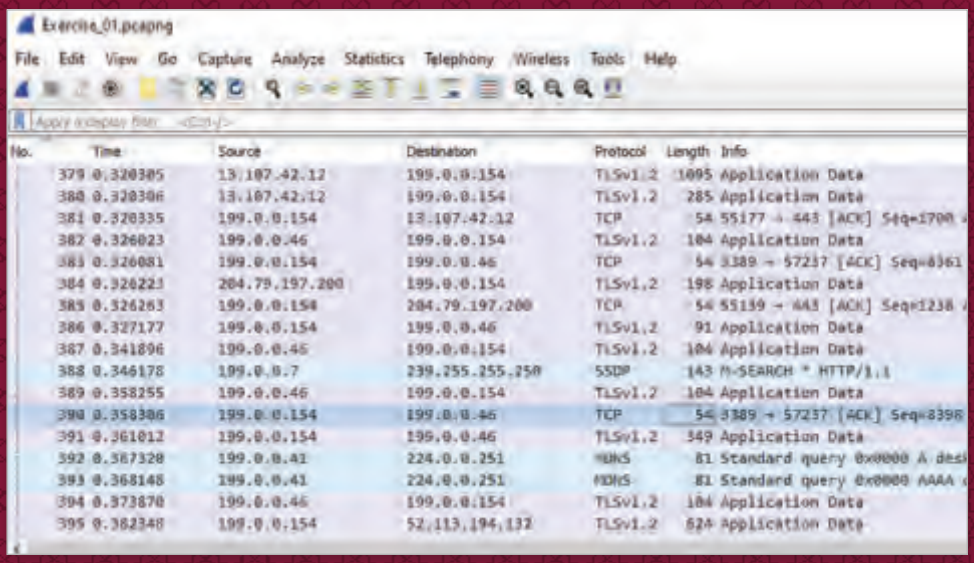
ابحث عن المعلومات التي ستساعدك في إنشاء قائمة التحقق.

استخدم **Microsoft Word** لإنشاء قائمة التحقق.

احفظ قائمة التحقق السابقة ثم أنشئ رسالة بريد إلكتروني موقعة رقميًا بواسطة **Microsoft Outlook**. قم بمشاركة هذه القائمة مع زملاءك بالفصل الدراسي.

مشروع الوحدة

العنوان: فحص نتائج المسح



الوصف: افتح ملف ممسوح مسبقاً لتقييم حركة المرور في الحزم الفردية التي تمر عبر بطاقة واجهة المستخدم للشبكة المعينة.

الأدوات: **Wireshark**

خطوات التنفيذ:

- افتح ملف المسح.
- استخرج أهم المعلومات من الحزم.
- حاول كشف النشاط المشبوه.

ماذا تعلمت

تعلمت في هذه الوحدة:

> ما هو أمن المعلومات ومدى أهميته.

> ما هي الجرائم الإلكترونية وما هي أنواعها.

> الاحتياطات اللازمة للحفاظ على أمننا الشخصي وأمن الحاسوب.

> جدار النار ودوره في حماية الحاسوب والشبكة من الاتصالات المشبوهة.

> أنواع الحسابات المتاحة في بيئة **Windows** واستخداماتها.

> الأذونات التي يمكن تعيينها للملفات والمجلدات في **Windows**.

> 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.

> الشهادة الرقمية ودورها في تأكيد هوية الأفراد والمؤسسات أثناء إجراء المعاملات المختلفة على الإنترنت.

> كيفية تبادل رسائل البريد الإلكتروني المشفرة والموقعة رقميًا.

> الشبكات الافتراضية الخاصة وكيفية استخدامها لتشفير وحماية البيانات المتبادلة عبر الشبكة.

> المقارنة بين أنظمة تشغيل أجهزة انترنت الأشياء وأنظمة تشغيل الحواسيب المكتبية.

> تحليل الحزم لرصد أنشطة المهاجمين وحماية الشبكة.

الدرس 1	الأمن الرقمي Cybersecurity	الجرائم الإلكترونية Cybercrimes	الاحتيال الإلكتروني Phishing scams
	أمن المعلومات Information security	التسلل الإلكتروني Cyberstalking	خرق الحماية Security breach
	انتهاك الخصوصية Invasion of Privacy	المضايقات عبر الإنترنت Online harassment	سرقة الهوية Identity theft

الدرس 2	الأمن الشخصي Personal cybersecurity	هجوم الفدية Ransomware	قائمة التحقق من أمن أجهزة الحاسوب Security checklist
	أمن الحاسوب Computer cybersecurity	البرمجيات الضارة Malware	التحقق الثنائي أو المتعدد Multi-factor Authentication

الدرس 3	جدار النار Firewall	حسابات Microsoft Microsoft accounts	أذونات المجلدات Folder permitions
	أجيال جُدر الحماية Firewall generations	الحسابات المحلية Local accounts	حسابات المستخدم User accounts
	أذونات الملفات File permissions		

الدرس 4	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		

الدرس 5	تشفير البريد الإلكتروني Email encryption	الشهادة الرقمية Digital certificate	المعرِّف الرقمي Digital ID
	التوقيع الرقمي Digital signature	نظام التشغيل Operating System OS	انترنت الأشياء Internet of Things IoT
	الشبكة الخاصة الافتراضية Virtual Private Network VPN	عميل الشبكة الخاصة الا فترا ضية VPN client	

الدرس 6	محلل الحزم Packet analyzer	التجسس على حزم البيانات Packet sniffing	نتائج المسح Scan results
	نشاط مشبوه Suspicious activity		

الصف	الصفحة	الملاحظة

الصف	الصفحة	الملاحظة

الصف	الصفحة	الملاحظة

الصف	الصفحة	الملاحظة

تكنولوجيا المعلومات المستوى الثاني عشر المسار التكنولوجي
الفصل الدراسي الثاني 2021 - 2020
كتاب الطالب

تم النشر بواسطة: **دار النشر MM Publications**
www.mmpublications.com
info@mmpublications.com
المكاتب
المملكة المتحدة، الصين، قبرص، اليونان، كوريا، بولندا، تركيا، الولايات المتحدة الأمريكية، الشركات المنتسبة والممثلين في جميع أنحاء العالم.

تم الإنتاج في الاتحاد الأوروبي

الرقم الدولي المعياري للكتاب: **978-618-05-5245-4** N2009002032-18112