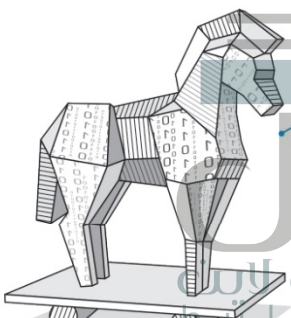
الدرس الخامس:

الاستخدام الآمن للإنترنت

إن الإمكانات التي توفرها شبكة الإنترنت مذهلة للغاية، فهي تجعل حياتك أسهل بكثير، فعلى سبيل المثال يمكنك من خلالها إنجاز واجباتك المدرسية بشكل أسرع والتواصل مع الآخرين والشراء والبيع وغيرها.

لكن رغم جميع تلك المزايا إلا انه باستخدامك شبكة الإنترنت الضخمة والمتنوعة يكون جهازك عُرضة بصورة دائمة لأخطار الفيروسات. فما المقصود **بفيروس الحاسب؟** هو برنامج خبيث يقوم بتكرار نفسه وينتشر من حاسب إلى آخر. الغرض الرئيس لهذا البرنامج هو أن يصيب جهاز الحاسب الخاص بك بالضرر سواء من خلال حذف الملفات أو سرقة المعلومات أو منع الحاسب من العمل بطريقة صحيحة. يتم إنشاء الفيروسات بواسطة أشخاص ذوي معرفة جيدة ببرمجة الحاسب والشبكات.

يُطلق مصطلح **البرامج الضارة** (Malicious programs) على فئة البرامج التي تهدف إلى تعطيل عملية تشغيل الحاسب، وتلك التي تجمع معلومات حساسة، أو تصل إلى أنظمة حاسوبية معينة. من أمثلة البرامج الضارة **برامج الديدان** (Worms)، و**برامج أحصنة طروادة** (Trojan Horses)، و**البرامج الدعائية** (Adware)، و**برامج التجسس** (Spyware)، **برامج الفدية الضارة** (Ransomware).

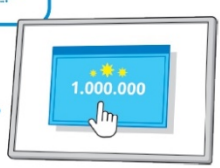


حصان طروادة (Trojan Horse) يبدو وكأنه برنامج طبيعي وغير ضار. والغرض منه هو منح المتسلل وصولًا غير مصرح به إلى جهاز الحاسب الخاص بك. أحصنة طروادة عادةً غير مبرمجة لنسخ نفسها أو إصابة ملفات أخرى ولكنها مبرمجة لسرقة المعلومات من جهازك.

برامج الدودة (Worm) تكرر نفسها من أجل الانتشار في أجهزة الحاسب الأخرى، وذلك غالبًا من خلال الانتشار عبر الشبكة.

برامج التجسس (Spyware) تجمع معلومات حول المستخدمين دون علمهم. وهي برامج مخفية عن المستخدم ويصعب اكتشافها.

برامج الفدية الضارة (Ransomware) تُعد أحد أشكال البرامج الضارة التي تقوم بتشفير ملفات المستخدم، ثم يطلب المهاجم مبلغًا كبيرًا من المال كفدية من الضحية لاستعادة الوصول إلى بياناته.



البرامج الدعائية (Adware) تُظهر الإعلانات دون إذن المستخدم، وذلك في الغالب على شكل نافذة منبثقة في واجهة المستخدم أو داخل أحد البرامج التي يستخدمها. قد تحتوي بعض الإعلانات على محتوى ضار.

الفيروسات

فيروسات الحاسب لا تكون عشوائية. ولا يعقل أن يصاب جهاز الحاسب الآلي بها فجأة وبدون سبب، ولكن هناك أسباب وطرق لإصابة جهاز الحاسب الآلي بالفيروسات، وفيما يلي قائمة بالطرق الشائعة لإنتشارها:

مرفقات البريد الإلكتروني

تُعدُّ رسائل البريد الإلكتروني من أكثر الطرق شيوعًا لإصابة جهاز الحاسب بالفيروسات أو البرامج الضارة. لا تفتح أبدًا رسالة بريد إلكتروني تلقيتها من شخص مجهول، وكذلك لا تفتح أي مرفق قبل ان تتأكد أنه من شخص تعرفه ولا يحتوي على فيروسات.

الوسائط القابلة للإزالة

عند توصيل بطاقة ذاكرة أو محرك أقراص USB أو أي نوع آخر من الوسائط القابلة للإزالة بجهاز الحاسب، فهناك احتمال نقل فيروس للحاسب من خلال هذه الوسائط. ففي حال إحتواء البرامج أو الملفات في هذه الوسائط على فيروس، فسيتم نقل هذا الفيروس إلى جهاز الحاسب عند توصيل الوسائط به.

تنزيلات الإنترنت

عند تنزيل أي محتوى من الإنترنت، فأنت بذلك تثبّت ملفات جديدة على جهاز الحاسب. حيث يكثر إرفاق العديد من من الفيروسات فيها. مثل بعض البرامج والألعاب غير المرخصة او التي يتم تحميلها بطريقة غير مشروعة.

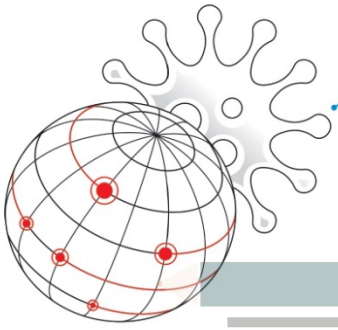
الإعلانات عبر الإنترنت

الإعلانات الضارة عبر الإنترنت هي مجرد طريقة أخرى يمكن أن يصاب بها جهاز الحاسب الخاص بك بالفيروس. غالبًا ما يضع المحتالون إعلانات نظيفة على مواقع الويب الموثوقة ويتركونها في مكانها لفترة من الوقت لاكتساب المصداقية. وبعد مرور بعض الوقت، يقومون بوضع كود ضار في الإعلان يصيب جهاز الحاسب الخاص بك عند الضغط عليه.

فيما يلي بعض النصائح التي يمكنك اتباعها لحماية جهاز الحاسب الخاص بك من فيروسات الحاسب:
ثبّت دائمًا برنامج مكافحة الفيروسات على جهاز الحاسب الخاص بك، احرص دائمًا على تشغيله وتأكد من حصولك على التحديثات بانتظام.
افحص أي وسائط قابلة للإزالة قبل فتح أي ملفات أو برامج فيها.
لا تضغط مطلقًا على أي رابط أو مرفق تتلقاه في رسالة بريد إلكتروني ما لم تكن متأكدًا من أنها واردة من شخص تعرفه وتثق به.
قم بعمل نسخة احتياطية لبيانات جهاز الحاسب الخاص بك وبشكل دوري مستمر، إذا أثر فيروس على جهاز الحاسب الخاص بك، فإن النسخ الاحتياطي للبيانات على محرك أقراص ثابت خارجي أو في السحابة يسمح لك باستعادة ما تحتاجه.
عندما تتلقى بريدًا إلكترونيًا من مصرف أو شركة ما ويُطلب فيه معلومات شخصية، فلا تضغط على الرابط. ربما يكون بريدًا إلكترونيًا مزيفًا يمكّن المرسل من سرقة معلوماتك أو إصابة نظامك بفيروس.

الرسائل الخطيرة

تقوم بعض رسائل البريد الإلكتروني المشبوهة بمحاولة جمع المعلومات عن المستخدم، وذلك بهدف استغلال جهازه للإعلانات التجارية.



تصنف بعض أنواع رسائل البريد الإلكتروني على أنها **بريد عشوائي** (Spam) أو **بريد غير هام** (Junk)، وهي ببساطة رسائل يتم إرسالها إلى آلاف الأشخاص في نفس اللحظة. قد تحتوي رسائل البريد العشوائي على برامج ضارة مرتبطة بها أو على روابط مشبوهة ترسلك إلى موقع ويب يحتوي على برامج ضارة.

رسائل الاحتيال (Phishing) تطلق على رسائل يتم إرسالها بغرض الوصول إلى المعلومات الشخصية كأسماء المستخدمين وكلمات المرور وأرقام بطاقات الائتمان. يتم ذلك عادةً بتوجيه المستخدم إلى موقع ويب وهمي ثم يُطلب من المستخدم كتابة جميع بياناته الشخصية.

سلسلة الرسائل

(Chain mail) تطلق على نوع من رسائل البريد الإلكتروني التي تُقنع المتسلم بإعادة توجيهها إلى مستخدمين آخرين مثل جهات اتصال المستخدم، وعادة ما تحتوي تلك الرسائل على قصص حزينة أو وصفٍ لأحداث درامية، وذلك بشكل يثير القارئ لمشاركتها، بينما تقوم الرسائل في الواقع بجمع المعلومات واستخدامها لاستهداف المستخدمين.

حماية الأجهزة

يجب تثبيت وتفعيل برنامج مكافحة الفيروسات على جهاز الحاسب الخاص بك مع التأكد من تحديثه باستمرار لضمان الكشف عن البرامج الضارة الجديدة. يمكنك شراء برنامج مكافحة فيروسات تجاري، ولكن إن لم ترغب بذلك فإن نظام **ويندوز** (Windows) يحتوي على **أمن الويندوز** (Windows Security) والذي يمكنه مساعدتك في حماية شبكتك المنزلية وتأمين بياناتك من تهديدات الإنترنت.

مكافحة الفيروسات

يبحث برنامج مكافحة الفيروسات بشكل مستمر عن البرامج الضارة. يمكنك أيضًا إجراء فحص للتأكد من أن جهاز الحاسب الخاص بك خالي من الفيروسات وآمن باتباع الخطوات التالية:

التحقق من وجود الفيروسات:

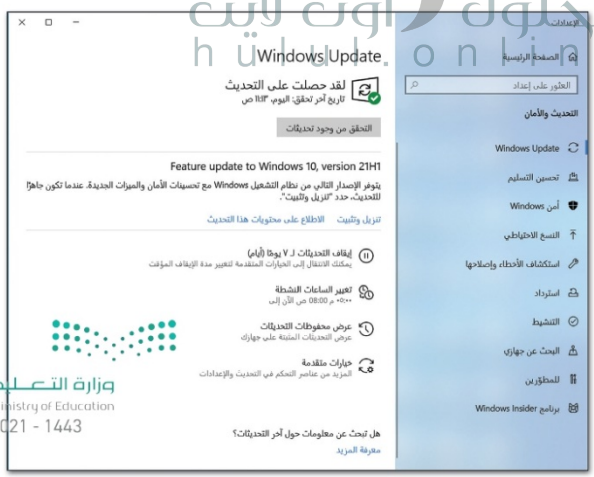
> اضغط على زر ابدأ (Start). 1

> مَرِّر الشريط الجانبي للأسفل ثم اضغط على **أمن Windows** (Windows Security). 2

> اضغط على **الحماية من أنشطة الفيروسات والتهديد** (Virus & threat protection)، 3 ثم اضغط على **فحص سريع** (Quick Scan). 4

طريقة تحديث برنامج مكافحة الفيروسات

يمكن لبرنامج مكافحة الفيروسات التحقق من البرامج الضارة التي يمكنه التعرف عليها، ويكمن التحدي الكبير في ظهور فيروسات بشكل مستمر، ولذلك من الضروري تحديث برنامج مكافحة الفيروسات باستمرار. يوجد في جميع برامج مكافحة الفيروسات زر للتحديث أو للتحقق من وجود تحديثات جديدة، وذلك عند الاتصال بالإنترنت.



أمور يجب الانتباه لها

يجب أن تُبْقِي جهاز الحاسب الخاص بك مُحدثًا دائمًا، فقد يحتاج نظام التشغيل والبرامج الملحقة إلى إجراء تحديثات معينة لتصحيح بعض المشاكل، لذلك وَافِق دومًا عليها.

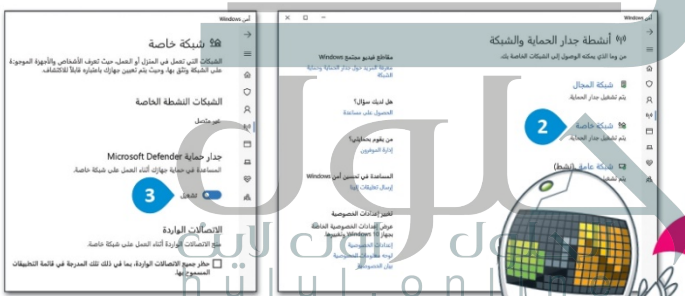
جدار الحماية (Firewall)

يمكن أن يكون جدار الحماية برنامجًا مستقلًا أو جهازًا منفصلًا، ويُستخدَم للمساعدة في الحفاظ على أمان الشبكة. إنه يتحكم في كيفية البيانات عبر الشبكة، ويحلل البيانات لتحديد ما إذا كان يُسمح لها بالدخول إلى الحاسب أم لا.

لتشغيل جدار الحماية وبندوز (Windows Firewall):

> في نافذة **أمن Windows** (Windows Security)، اضغط على **أنشطة جدار الحماية والشبكة** (Firewall & Network Protection). 1

> اختر ملف تعريف شبكة مثل **شبكة خاصة** (Private network)، 2 ثم ضمن **جدار حماية Microsoft Defender** (Microsoft Defender Firewall)، بدِّل الإعداد إلى **تشغيل** (On). 3



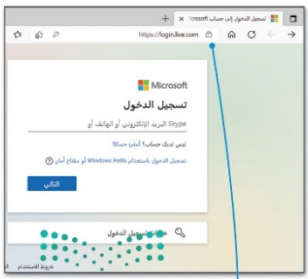
لا يُنصح بإيقاف تشغيل جدار الحماية، فالفيروسات تبحث باستمرار عن بوابة للتسلل إلى جهاز الحاسب من خلال الشبكة. لا تقلق حول ألعابك عبر الإنترنت، فعندما يحتاج برنامج ما الوصول إلى الإنترنت فسيطلب منك الإذن للقيام بذلك، وسيمنحه إياه جدار الحماية.

الاتصال الآمن

هناك طريقة أخرى لتجنب الإصابة بالفيروس وهي زيارة مواقع الويب الآمنة والموثوق بها. على سبيل المثال: إذا كنت ترغب في شراء منتج ما، فانتقل إلى أي متجر إلكتروني توجد طريقة للتحقق من موثوقية الموقع من خلال ظهور رمز القفل بجانب اسم موقع الويب في شريط العنوان.

عندما يظهر رمز القفل، يتم تشفير كل الاتصالات بينك وبين الموقع. وبعبارة بسيطة، إذا كتبت كلمة مرور البريد الإلكتروني وكانت على سبيل المثال 3x@mple، سيتم نقلها بصورة wrt93is0932959dsfwsdf34sfsrq3، لذلك لا يمكن لأحد فهمه باستثناء جهاز الحاسب الخاص بك وخادم الموقع.

هل يعني هذا أنه عند رؤية رمز القفل يمكن كتابة أي نوع من المعلومات؟ بالطبع لا، يجب عليك التأكد من موثوقية موقع الويب الذي ستشارك عليه معلوماتك الشخصية.



أخبر أصدقاءك بأهمية رمز القفل، خصوصًا عند تسوقهم عبر الإنترنت.

أسماء المستخدمين وكلمات المرور

في كل مرة تتعامل بها مع حساب على الإنترنت يُطلب منك تسجيل الدخول وكلمة مرور. لماذا يُعدُّ الأمر مُهمًا وما مدى حاجتنا إلى التسجيل؟

تحتاج إلى حماية بياناتك على الإنترنت حتى لا يصل إليها الآخرون، على سبيل المثال: لابد من وجود حساب شخصي خاص بك لكي يتعرف عليك أصدقاؤك على الإنترنت. من الممكن أن يكون اسم المستخدم الخاص بك اسمك الحقيقي أو لقبك، وكذلك فأنت بحاجة إلى كلمة مرور سرية تعرفها أنت وحدك وربما تشاركها مع والديك.

لتركيب يمكننا إنشاء كلمة مرور قوية:

- يجب أن تكون كلمة المرور طويلة بما فيه الكفاية. من السهل جدًا كشف كلمة المرور المكونة من 4 أحرف. حاول استخدام كلمات المرور التي يتراوح طولها من 8 إلى 10 أحرف على الأقل.
- تجنب الكلمات الشائعة مثل، أمي، أبي، اسم عائلتك وغيرها.
- لا تستخدم نفس الكلمة / العبارة لكل من اسم المستخدم وكلمة المرور الخاصة بك. لا تستخدم أيضًا المعلومات الشخصية: يوم ميلادك، فريقك المفضل، رقم هاتفك، إلخ.
- استخدم الرموز والأرقام معًا، فمن الصعب تخمين كلمة مرور مثل **chicken5meal7#** مقابل كلمة المرور **chickenmeal** حيث يسهل تخمينها.
- إن إحدى الطرق السهلة لإنشاء كلمات مرور قوية يمكنك تذكرها هي التفكير في كلمة أو عبارة واستبدال حروف العلة بالرموز والأرقام. على سبيل المثال، بدلاً من **saudiarabia**، جرّب **!Saudi&Arabia**. من الصعب تخمين هذه الكلمات ولكن يمكنك تذكرها بسهولة.
- إذا كنت تستخدم حسابًا مهمًا، فغيّر كلمة المرور الخاصة بك باستمرار لكل فترة زمنية تتراوح بين 6 و 12 شهر.

نصيحة ذكية

لا تستخدم كلمة المرور نفسها في عدة أماكن، فإذا اكتشفها شخصٌ ما فسيتمكن من الوصول إلى جميع حساباتك. ولا تكتب كلمة المرور في ورقة خارجية أو تتركها مكتوبة بجانب جهاز الحاسب الخاص بك.

لنطبق معًا

تدريب 1

بمساعدة معلمك اشترك مع ثلاثة أو أربعة من زملائك وأجب عن الأسئلة التالية مستعينًا بكتابك أو الإنترنت:

> ما هي البرامج الضارة؟

هي فئة من البرامج تهدف إلى تعطيل تشغيل الحاسب أو جمع معلومات حساسة أو الوصول إلى أنظمة الحاسب.

> ما هو برنامج حصان طروادة؟

حصان طروادة يبدو في ظاهرة بأنه غير ضار، في حين أنه يهدف في الحقيقة إلى منح المتسلل وصولاً غير مصرح به إلى جهاز الحاسب. أحصنة طروادة عادة غير مبرمجة لنسخ نفسها أو إصابة ملفات أخرى ولكنها مبرمجة لسرقة المعلومات من أجهزة الحاسب.

> ما هي برامج التجسس؟

برامج التجسس تجمع معلومات حول المستخدمين دون علمهم، وتتميز بكونها برامج مخفية عن المستخدم ويصعب اكتشافها.

> ما هو برنامج مكافحة الفيروسات؟

هو برنامج حاسب يستخدم لمنع البرامج الضارة واكتشافها وإزالتها.

> ما هو جدار الحماية؟

جدار الحماية أو (جدار النار) هو برنامج ثابت يمنع الوصول غير المصرح به إلى الشبكة ويقوم بفحص حركة البيانات الواردة والصادرة في الشبكة باستخدام مجموعة من القواعد لتحديد التهديدات ومنعها.

> ما أهمية رمز القفل؟

رمز القفل هو وسيلة للتحقق مما إذا كان موقع الويب موثوقاً من عدمه.

تدريب 2

استخدام مكافح الفيروسات.

برنامج مكافحة الفيروسات يقوم بفحص جهاز الحاسب الخاص بك باستمرار بحثًا عن البرامج الضارة. اقرأ التعليمات التالية ثم أكمل الإجابة مكان النقاط أدناه:

ابحث في جهاز الحاسب الخاص بك عن برنامج مكافحة الفيروسات لديك ثم اكتب اسمه:

.....

إسأل معلمك إذا كان قد اشترى برنامج مكافحة الفيروسات أو قام بتنزيله من الويب:

.....

- ابحث عنه ثم إفتحه.
- افحص جهاز الحاسب الخاص بك بحثًا عن البرامج الضارة.
- هل وجدت فيروسات أو برامج تجسس؟

.....

- إذا كانت الإجابة نعم، إسأل معلمك عن طريقة التخلص منها.

تدريب 3

البحث عن الفيروسات.

لا يكفي مجرد تثبيت برنامج مكافحة فيروسات على جهاز الحاسب الخاص بك، حيث تظهر فيروسات جديدة بشكل مستمر، ولذلك يجب تحديث برنامج مكافحة الفيروسات الخاص بك باستمرار. اقرأ التعليمات التالية ثم املأ الفراغات أدناه:

تأكد من أن لديك اتصال بالإنترنت ثم حَدِّث برنامج مكافحة الفيروسات الخاص بك.

- افحص الآن جهاز الحاسب الخاص بك مرة أخرى.
- هل وجدت أي فيروسات أو برامج تجسس؟ .....
- ما الذي استنتجته؟.....

تدريب 4

إنشاء كلمة مرور قوية

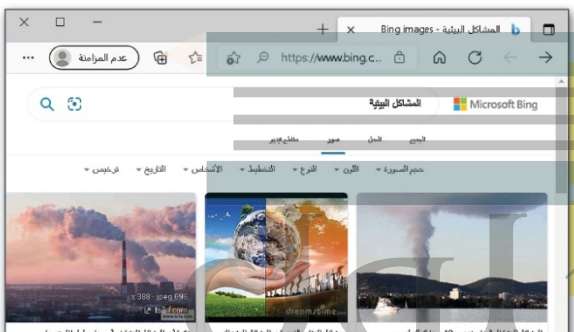
هناك العديد من طرق الحماية من مخاطر الويب. يمكنك حماية معلوماتك الشخصية باستخدام أسماء المستخدم وكلمات المرور التي لا يستطيع أحد اكتشافها أو استخدامها. ابحث في الويب واكتب (بعض الإرشادات التي يجب اتباعها من أجل إنشاء اسم مستخدم وكلمة مرور آمنة):

الإرشادات لكتابة اسم المستخدم وكلمة المرور:

- يجب أن تكون كلمة المرور طويلة (من 8 إلى 10 أحرف على الأقل).
- تجنب الكلمات الشائعة والمعلومات الشخصية.
- عدم استخدام نفس كلمة المرور واسم المستخدم في كل موقع ويب.
- استخدام الرموز والأرقام وأحرف كبيرة وصغيرة.
- تغيير كلمة المرور مرتين كل عام على الأقل.
- عدم إخبار أي أحد سوى الوالدين بكلمات مرورك.

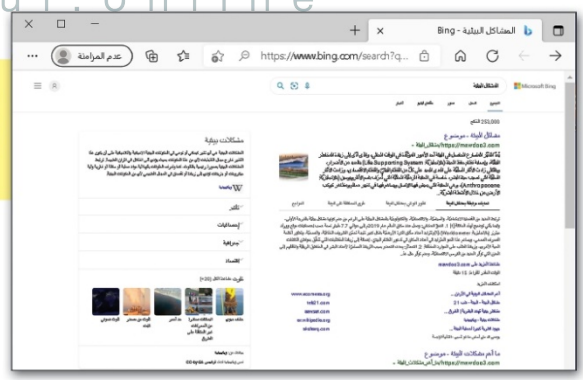
مشروع الوحدة

بالتنسيق مع معلمك ، شكّل مجموعة من زملائك في الصف. سيقوم باقي الطلبة بتشكيل مجموعات مماثلة بحيث تقوم كل مجموعة بالتحضير لموضوع يتعلق بالبيئة. عليكم أن تضعوا بعض الملصقات على الجدران حول جميع المشاكل البيئية التي يواجهها العالم اليوم. اجمعوا الصور والملصقات الصغيرة التي تصف المشكلة وحلولها الممكنة، ويمكن إضافة آرائكم الخاصة حول ذلك.



تستطيع **المجموعة الأولى** الاستعانة بالإنترنت، ولكن يتعين على **المجموعة الثانية** استخدام الطريقة التقليدية.

يمكن **للمجموعتين** الاستعانة بالويب للعثور على بعض الصور.



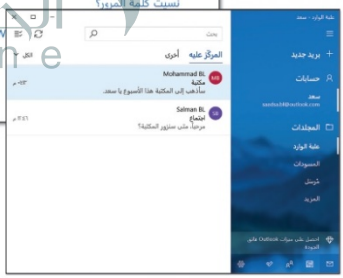
ستبحث **المجموعة الأولى** عن المعلومات عبر الإنترنت، بينما ستقوم **المجموعة الثانية** بالبحث في الكتب.

وزارة التعليم
Ministry of Education
2021 - 1443

اعرضوا عملكم أمام زملائكم في الصف وادعوا الآخرين لمشاهدة هذا العرض التقديمي.

ستستخدم **المجموعة الأولى** رسائل البريد الإلكتروني وأي وسيلة أخرى للاتصال عبر الإنترنت.

يمكن **للمجموعة الثانية** استخدام الهاتف والرسائل البريدية فقط.

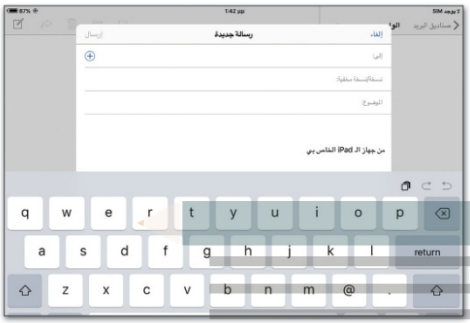


بعد الانتهاء من تنفيذ المشروع، ناقشوا الصعوبات التي واجهتكم معًا، مع محاولة فهم مساهمة التقنية في جعل حياتنا أسهل، وناقشوا كذلك الآثار السلبية للتقنية على البيئة، وكيف يمكن توظيف التقنية دون الإضرار بالبيئة.

برامج أخرى

بريد أبل (Apple Mail)

يتوفر برنامج **بريد أبل** على جميع أجهزة **آي باد** (iPad) و**آيفون** (iPhone). يمكن إنشاء بريد إلكتروني واستخدام البرنامج على هذه الأجهزة بسهولة. وهكذا يمكنك تلقي رسائل بريدك الإلكتروني على جهاز آيفون الخاص بك، وإذا كان لديك جهاز آي باد فستجد الرسائل ذاتها قد تم تلقيها عليه أيضًا.

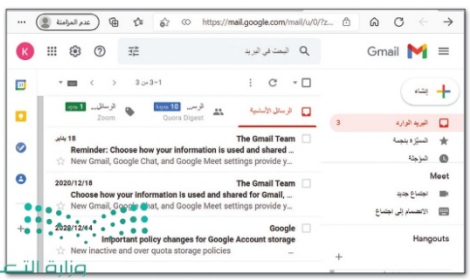


بريد جوجل أندرويد (Google Android Mail)

تمامًا مثل **أبل**، لدى جميع أجهزة **أندرويد** (Android) برنامج بريد إلكتروني بحيث يمكنك إنشاء حساب واستخدامه. علمًا بأن جميع برامج البريد لها نفس الوظائف الرئيسة. فإذا كنت تتقن واحدة منها فيمكنك بسهولة استخدام جميع برامج البريد الإلكتروني الأخرى.

جوجل جي ميل (Google Gmail)

بريد إلكتروني قائم على الويب. يمكنك إنشاء حساب والوصول إليه باستخدام متصفح الويب. لا تحتاج إلى تثبيت أي برنامج على جهاز الحاسب الخاص بك، الشيء الوحيد الذي تحتاجه هو متصفح ويب واتصال بالإنترنت.



في الختام

جدول المهارات

المهارة	درجة الإتقان	
	أتقن	لم يتقن
1. تصفح الإنترنت.		
2. البحث عن المعلومات في الإنترنت.		
3. نسخ نص أو صورة من الإنترنت.		
4. إضافة موقع ويب إلى المُفضلة.		
5. إرسال واستقبال رسالة بريد إلكتروني.		
6. الرد على رسالة من مُرسل واحد أو أكثر.		
7. إرفاق الملفات إلى رسالة بريد إلكتروني.		
8. التدقيق الإملائي لرسائل البريد الإلكتروني.		
9. إعادة توجيه رسالة بريد إلكتروني.		
10. حماية جهاز الحاسب من الفيروسات.		

المصطلحات

Adware	إعلانات	Network	الشبكة
Address Book	دفتر العناوين	Padlock	قفل
Address Bar	شريط العناوين	Phishing	الرسائل الاحتيالية
Attach	إرفاق	Ransomware	برامج الفدية الضارة
Calendar	تقويم	Reply	الرد
Cc	نسخة	Spyware	برامج التجسس
Firewall	جدار الحماية	Spam	بريد عشوائي
Flag	علامة	Tabs	علامات التبويب
Home page	الصفحة الرئيسة	User name	اسم مستخدم
Hyperlink	ارتباط تشعبي	Website	موقع ويب
Inbox	علبة الوارد	Web Page	صفحة ويب
Internet	الإنترنت	Web Browser	متصفح ويب
Malicious Program	برنامج ضار	Web Address	عنوان ويب
Online	عبر الإنترنت	Worm	دودة