الوحدة 2 الدرس 2

الأمن الشخصي والحاسوب

وصف الدرس

الغرض العام من هذا الدرس أن يتعرف الطلبة على طرق حماية معلوماتهم الشخصية وأنظمة حواسيبهم.

ما سيتعلمه الطالب

> أهم احتياطات الأمن الشخصي.

> كيفية الوقاية من البرمجيات الضارة، وكشفها وإزالتها.

نتاجات التعلم

> الاحتياطات اللازمة للحفاظ على أمننا الشخصي وأمن الحاسوب.

المصطلحات

اللغة العربية	اللغة الإنجليزية
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

التحديات المتوقعة

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.

ومن 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.

126

> قد يجد بعض الطلبة صعوبة في فهم مدى سهولة سرقة المعلومات الشخصية من قِبل المتسللين. اشرح الأسباب المتعددة التي تدفع هؤلاء المتسللين لعمل ذلك، سواء لسرقة المعلومات أو لتسريبها أو لأغراض الابتزاز المالي. أخبر الطلبة أن هناك تاريخًا طويلًا لعمليات الاختراق والتي لم تتوقف يومًا بل تطورت وازدادت حدتها وتأثيرها سواء على الأفراد أو الشركات التجارية أو حتى المؤسسات الحكومية، ولذلك يجب أن يكون الجميع مستعدًا لمثل هذا الخطر.

> قد يجد بعض الطلبة صعوبة في فهم حاجتهم إلى تحديث تطبيقاتهم وخاصةً عند اعتيادهم على استخدام إصدار معين من تطبيق ما. وضِّح للطلبة أن عملية تحديث نظام تشغيل حواسيبهم أو تطبيقاتهم تساهم في تقليل مخاطر اختراق الأجهزة وذلك لأن نظام التشغيل أو التطبيق غير المُحدث باستمرار قد يحتوي على العديد من الثغرات الأمنية.

> قد لا يدرك بعض الطلبة أنهم قد يتلقون رسائل إلكترونية تطلب منهم بعض المعلومات الشخصية ممن يدَّعون بأنهم إحدى الجهات الرسمية كالبنك مثلًا. اشرح للطلبة أنه لا ينبغي عليهم فتح مثل هذه الرسائل، وكذلك عليهم عدم الرد عليها وتجنب الضغط على أي رابط تشعبي داخل الرسالة، حيث يمكن المرور بالمؤشر فوق الارتباط التشعبي دون الضغط عليه للحصول على المعاينة، والتي ستظهر على الشاشة لموقع الارتباط التشعبي، ثم مقارنة ذلك بعنوان موقع الويب الحقيقي للبنك. يجب عدم مشاركة أية معلومات شخصية مهما كانت حيث يمكن أن يتيح ذلك أيضاً تعرض حاسوبك للهجوم.

> عادة ما يقوم الطلبة بالتسجيل في مواقع الويب التعليمية المختلفة بنفس اسم المستخدم وكلمة المرور، وذلك بطبيعة الحال لتفادي نسيان معلومات الدخول. وضِّح للطلبة أن عليهم استخدام اسم مستخدم وكلمة مرور مختلفين في كل موقع أو نظام يقومون بالتسجيل به، وبالتالي إذا تمكن أحد ما من الحصول على معلومات تسجيل دخول أحد المواقع، فلن يتمكن من تسجيل الدخول لبقية الحسابات. يمكنك أن تقترح استخدام مدير كلمات المرور.

> قد يعتقد بعض الطلبة أن إجراء النسخة الاحتياطية لبيانات حواسيبهم على محرك أقراص ثابت خارجي يُعدُّ كافيًا. اشرح للطلبة أن هذه الطريقة لا تعدُّ كافية لأن مثل هذا الجهاز قد يفشل لعدة أسباب كوجود خطأ في عملية النسخ أو لحدوث عطل في الأجهزة، أو تلف البرامج المثُبتة، أو ارتفاع الحرارة، أو خطر الماء أو مشاكل الطاقة والحوادث، وبالتالي سيفقدون بياناتهم. لهذا السبب يتعين عليهم إنشاء النسخ الاحتياطية بواسطة التخزين السحابي.

> قد يواجه بعض الطلبة صعوبة في فهم ضرورة تجنب الاتصال بالإنترنت من خلال شبكات **Wi-Fi** العامة. اشرح للطلبة أن هذا النوع من الاتصال يمنح المتسلل إمكانية الوصول والتجسس على أي معلومات يتم تبادلها بينهم وبين مواقع الويب التي يزورونها، بما فيها تفاصيل أنشطة التصفح وتسجيلات الدخول إلى الحسابات ومعاملات الشراء، وقد يتمكن المتسللون من التحكم الكامل بالحواسيب دون التمكن من فعل أي شيء لإيقافهم.

> قد يجد بعض الطلبة صعوبة في فهم ضرورة تنزيل التطبيقات من مواقعها الرسمية فقط. اشرح للطلبة أن مواقع الويب التي توفر تطبيقات من شركات أخرى قد تحتوي على برمجيات مشبوهة أو فيروسات.

> قد لا يكون بعض الطلبة على دراية بما يطلق عليها ببرمجيات هجوم الفدية، ولربما يكونون قد وقعوا ضحية لها في الماضي. اشرح للطلبة أن عليهم تثبيت تطبيق برامج مكافحة البرمجيات الضارة على حواسيبهم لتجنب ذلك، أما إذا كانوا ضحية لمثل هذا الأمر فعليهم إبلاغ السلطات المختصة وطلب المساعدة وعدم دفع أية فدية.

التمهيد

> مهِّد لغرض هذا الدرس بإثارة دافعية الطلبة في تعلم كيفية حماية معلوماتهم الشخصية وأنظمة حواسيبهم.

> يمكنك البدء بطرح بعض الأسئلة على الطلبة على سبيل المثال لا الحصر:

- لقد تعرفتم في الدرس السابق على الهجمات الإلكترونية. هل يمكنكم تحديد ببعض الخطوات التي يمكنكم اتخاذها لحماية أنفسكم بناءً على تجربتكم الحاسوبية السابقة؟
- هل تتم عملية القرصنة على أجهزة الحاسوب فقط أم أنها يمكن أن تحدث على الأدوات الإلكترونية الأخرى كالهاتف المنزلي الأرضي مثلًا؟
- ما هو التطبيق الذي يمكنكم استخدامه لتشفير جميع أسماء المستخدمين وكلمات المرور التي تستخدمها على مواقع الويب المختلفة؟
- هل تعتقدون بأن النسخ الاحتياطي لملفات حواسيبكم على قرص صلب خارجي يُعدُّ كافيًا؟
- هل تستخدمون شبكات **Wi-Fi** العامة؟ هل تدركون المخاطر التي قد تواجهونها؟ ما هي بعض تلك المخاطر؟
- ما المقصود بالبرامج الضارة، وكيف يمكنكم حماية أجهزتكم منها؟

- كيف يمكنكم معرفة ما إذا كان حاسوبكم مصابًا ببرامج ضارة بناءً على خبرتكم الحاسوبية؟
- هل تعرفون ما عليكم فعله في حال إصابة حواسيبكم بالبرامج الضارة؟
- هل تعرفون ما هو هجوم الفدية؟
- كيف تعتقدون بأنه يمكنكم حماية أنفسكم من برامج الفدية الضارة؟
- ما الذي يتوجب عليكم فعله للتأكد من أن حواسيبكم آمنة؟

التلميحات الخاصة بالتنفيذ

> ابدأ بشرح موضوع الدرس للطلبة بخصوص أمن المعلومات والحواسيب.

> اشرح للطلبة بعد ذلك وبالاستعانة بإرشادات كتاب الطالب الخطوات التي يتعين عليهم اتباعها لحماية أنفسهم من أي هجمات إلكترونية.

> استمر بشرح مفهوم البرامج الضارة للطلبة بالاستعانة بكتاب الطالب، مع شرح طرق حماية أنفسهم من تنزيل البرامج الضارة.

> اشرح للطلبة كيفية تحديد إصابة حواسيبهم بالبرامج الضارة، وما يجب عليهم فعله للتعامل مع هذا الأمر.

> استمر بشرح المقصود ببرامج الفدية وكيف يمكن حماية الحواسيب من خطرها.

> في النهاية استعن بإرشادات كتاب الطالب لتشرح للطلبة كيف يمكنهم التحقق من أن حواسيبهم آمنة.

استراتيجيات غلق الدرس

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

> هل تستطيع أن تتذكر:

- لماذا يتم اعتراض المعلومات الشخصية؟
- ما الذي يجب عليكم القيام به لحماية أنفسكم من الهجمات الإلكترونية؟
- ما هي البرامج الضارة؟
- ما الذي يجب عليكم فعله لحماية حواسيبكم أثناء التنزيل من البرامج الضارة؟
- كيف يمكنكم اكتشاف إصابة حواسيبكم بالبرامج الضارة؟
- ما الذي يجب فعله في حال إصابة نظام الحاسوب بالبرامج الضارة؟
- ما هي برامج هجوم الفدية؟
- كيف يمكن التحقق مما إذا كانت حواسيبكم آمنة؟

> ذكّر الطلبة بالمصطلحات الهامة وكرّرها معهم.

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

التدريبات المقترحة لغلق الدرس

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

الصف الثاني عشر | الفصل الأول | كتاب الطالب | صفحة 130

الفروق الفردية

تمارين إضافية للطلبة ذوي التحصيل المرتفع

> بعد الانتهاء من تنفيذ التمرين الثاني، اطلب من الطلبة تدوين ما سيفعلونه في حال إصابة حواسيبهم بالبرامج الضارة.

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 وتاريخ 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 أربعة من الإجراءات المتبعة للوقاية من البرمجيات الضارة.

.1 _____

.2 _____

.3 _____

.4 _____

133

الإجابات النموذجية للتدريبات

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 وتاريخ 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 أربعة من الإجراءات المتبعة للوقاية من البرمجيات الضارة.

1. تثبيت وتحديث برنامج الحماية من البرمجيات الضارة، واستخدام جدار الحماية.

2. انتبه لتحذيرات الأمان الخاصة بالمتصفح.

3. بدلاً من الضغط على ارتباط في بريد إلكتروني، اكتب عنوان URL لموقع موثوق مباشرة في المتصفح.

4. لا تفتح المرفقات في رسائل البريد الإلكتروني إلا إذا كنت تعرف المرسل.

3

اشرح أربعة من الإجراءات المتبعة للحفاظ على الأمن الإلكتروني الشخصي.

1. 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.

2. 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.

3. النسخ الاحتياطي الدوري للبيانات Backup. يُعدُّ 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.

4. تجنَّب 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 يُصعِّب على القراصنة الوصول إلى بياناتنا على الإنترنت، كما يوصى باستخدام الشبكة الخلوية عند عدم وجود شبكة VPN وذلك للحصول على مستوى أعلى من الأمان.

4 اذكر ثلاثة من الإحتياطات التي ينصح بها للوقاية من الجرائم الإلكترونية.

1. **التحديث الدوري للبرامج.**
2. **استخدام مضاد الفيروسات Antivirus وجدار الحماية Firewall.**
3. **استخدام كلمات المرور القوية وأدوات إدارة كلمات المرور.**

5 اشرح ما يجب عليك اتخاذه في حال الاشتباه بوجود البرمجيات الضارة على حاسوبك.

1. **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.**
2. **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.**
3. **التحقق من المتصفح لمعرفة ما إذا كان به أدوات لحذف البرامج الضارة، ومن الممكن أيضًا إعادة تعيين المتصفح إلى إعداداته الافتراضية.**
4. **الاستعانة بالدعم الفني من خلال الاتصال بالشركة المصنِّعة لجهازك، جهز الرقم التسلسلي قبل الاتصال بالشركة المصنعة للحاسوب، وتأكد من معرفتك للبرامج التي تم تثبيتها ومن قدرتك على تقديم وصف موجز للمشكلة.**

6

وضح المقصود بكل من:

> التحقق الثنائي أو المتعدد:

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.

> هجوم الفدية (الإبتزاز المالي):

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.