Cyber Security
الأمن الإلكتروني

Module One: Review Questions

1) Cyberspace refers to which of the following?
   a) Computer-to-computer activity
   b) Individual-to-individual activity
   c) Supervisor-to-employee activity
   d) Computer-to-physical location activity

مراجعة الوحدة الأولى

1) يشير الفضاء الإلكتروني إلى أي مما يلي؟
   أ) نشاط الكمبيوتر إلى الكمبيوتر
   ب) النشاط الفردي
   ج) نشاط من مشرف إلى موظف
   د) نشاط من موقع إلى آخر

2) What is an item that is included in cyberspace?
   a) Network
   b) Software
   c) Application
   d) All of the above

2) ما هو البند الذي يتم تضمينه في الفضاء الإلكتروني؟
   أ) شبكة
   ب) برمجيات
   ج) تطبيق
   د) كل ما سبق

3) Why is cyber security implemented?
   a) To speed up the network of a company's computers
   b) To avoid the disruption of a company's business
   c) To increase the number of clients a company has
   d) To lessen the number of employees a company employs

3) لماذا يتم تنفيذ الأمن السيبراني؟
   أ) لتسريع شبكة أجهزة الكمبيوتر الخاصة بالشركة
   ب) لتجنب تعطيل أعمال الشركة
   ج) لزيادة عدد العملاء لدى الشركة
   د) لتقليل عدد الموظفين الذين توظفهم الشركة

4) Cyber security helps control physical access to and prevents danger that may come in from:
   a) Hardware
   b) Network access

4) يساعد الأمن السيبراني على التحكم في الوصول المادي إلى الخطر الذي قد يأتي من :
   أ) الأجهزة
   ب) الوصول إلى الشبكة
   ج) حقن الشفرة

c) Code injection
d) All of the above

د) كل ما سبق

5) What type of information is NOT secure information that is likely to be compromised in a data security breach?
a) Intellectual property
b) Credit card information
c) The name of a company's CEO
d) Social security numbers

5) ما هو نوع المعلومات غير الآمنة التي من المحتمل أن تتعرض للخطر في خرق أمان البيانات؟
أ) الملكية الفكرية
ب) معلومات بطاقة الائتمان
ج) اسم الرئيس التنفيذي للشركة
د) أرقام الضمان الاجتماعي

6) What is the main purpose of computer sabotage?
a) To disable a company's computers or networks to prevent it from conducting business.
b) To disable a company's computers or networks to prevent it from being able to obtain a business license.
c) To disable a company's computers or networks to prevent it from being able to hire employees.
d) To disable a company's computers or networks to prevent it from being able to give its employees raises.

6) ما هو الغرض الرئيسي من تخريب الكمبيوتر؟
أ) لتعطيل أجهزة الكمبيوتر أو الشبكات الخاصة بالشركة لمنعها من القيام بأعمال تجارية.
ب) لتعطيل أجهزة الكمبيوتر أو الشبكات الخاصة بالشركة لمنعها من الحصول على ترخيص عمل.
ج) لتعطيل أجهزة الكمبيوتر أو الشبكات الخاصة بالشركة لمنعها من توظيف الموظفين.
د) لتعطيل أجهزة الكمبيوتر أو الشبكات الخاصة بالشركة لمنعها من أن تكون قادرة على منح موظفيها زيادات.

7) Why do "grey hat" hackers typically hack into computers?
a) To steal data for monetary gain
b) For the fun of it

7) لماذا "قبعة رمادية" قراصنة الاختراق عادة في أجهزة الكمبيوتر؟
أ) لسرقة البيانات لتحقيق مكاسب مالية
ب) للمتعة من ذلك

c) To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them

d) To sell data for monetary gain

ج) للعثور على نقاط الضعف في نظام الكمبيوتر حتى تتمكن الشركة من إصلاحها قبل أن يتمكن المتسللون ذوي النوايا السيئة من استغلاله

د) لبيع البيانات لتحقيق مكاسب نقدية

8) Why do “white hat” hackers typically hack into computers?

a) To steal data for monetary gain

b) For the fun of it

c) To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them

d) To sell data for monetary gain

8) لماذا قراصنة "قبعة بيضاء" عادة الاختراق إلى أجهزة الكمبيوتر؟

أ) لسرقة البيانات لتحقيق مكاسب مالية

ب) للمتعة من ذلك

ج) للعثور على نقاط الضعف في نظام الكمبيوتر حتى تتمكن الشركة من إصلاحها قبل أن يتمكن المتسللون ذوي النوايا السيئة من استغلالها

د) لبيع البيانات لتحقيق مكاسب نقدية

9) The method(s) of cyber security that a company uses should be tailored to fit the needs of the _____.

a) Hacker

b) Employees

c) Organization

d) Manager

9) يجب أن تكون طريقة (أساليالأمن السيبراني التي تستخدمها الشركة مصممة لتناسب احتياجات._____

أ) هاكر

ب) الموظفين

ج) التنظيم

د) المدير

10) _____ is the environment where computer transactions take place.

a) An office

b) Cyberspace

c) A mall

d) None of the above

10) _____هي البيئة التي تتم فيها معاملات الكمبيوتر.

أ) مكتب

ب) الفضاء السيبراني

ج) مول

د) لا شيء مما سبق

Module Two: Review Questions

1) How do worms work?
   a) They are always downloaded as email attachments
   b) They are automatically installed on every computer
   c) They must attach themselves to existing programs in order to spread
   d) They reproduce themselves to infect other computers

مراجعة الوحدة الثانية

1) كيف تعمل الديدان؟
   أ) يتم تنزيلها دائما كمرفقات بريد إلكتروني
   ب) يتم تثبيتها تلقائيا على كل جهاز كمبيوتر
   ج) يجب أن يعلقوا أنفسهم على البرامج القائمة من أجل الانتشار
   د) أنها تستنسخ نفسها لتصيب أجهزة الكمبيوتر الأخرى

2) Which of the following does the lesson NOT list as damage that worms can cause?
   a) Bandwidth consumption
   b) Immobilizing Safe Mode
   c) Corrupting files
   d) Stopping active anti-malware service

2) أي مما يلي لا يسرد الدرس كضرر يمكن أن تسببه الديدان؟
   أ) استهلاك عرض النطاق الترددي
   ب) تعطيل الوضع الآمن
   ج) تلف الملفات
   د) إيقاف خدمة مكافحة البرامج الضارة النشطة

3) When can infected files infect other computers?
   a) When the file is shared with other computers

3) متى يمكن للملفات المصابة أن تصيب أجهزة كمبيوتر أخرى؟
   أ) عند مشاركة الملف مع أجهزة كمبيوتر أخرى
   ب) ما إذا كان الملف مشتركا مع أجهزة كمبيوتر أخرى أم لا

b) Whether or not the file is shared with other computers
c) They automatically infect other computers within the same network of the originally infected computer
d) Never

ج) أنها تصيب تلقائيا أجهزة الكمبيوتر الأخرى داخل نفس الشبكة من الكمبيوتر المصاب أصلا
د) أبدا

4) Which of the following does the lesson NOT list as damage that viruses can cause?
a) Computer slowdown
b) Corrupting files
c) Taking over basic functions of the operating system
d) Bandwidth consumption

4) أي مما يلي لا يشمل الأضرار التي يمكن أن تسببها الفيروسات؟
أ) تباطؤ الكمبيوتر.
ب) تلف الملفات.
ج) تولي الوظائف الأساسية لنظام التشغيل.
د) استهلاك عرض النطاق الترددي.

5) Spyware is commonly used to bombard the user with:
a) Emails without attachments
b) Unsolicited text messages
c) Emails with attachments
d) Pop-up ads

5) يستخدم عادة برامج التجسس لقصف المستخدم مع:
أ) رسائل البريد الإلكتروني بدون مرفقات
ب) رسائل نصية غير مطلوبة
ج) رسائل البريد الإلكتروني مع المرفقات
د) الإعلانات المنبثقة

6) Which of the following does the lesson NOT list as damage that Spyware can cause?

6) أي مما يلي لا الدرس لا قائمة كما الضرر الذي يمكن أن يسبب برامج التجسس؟
أ) تحطم الكمبيوتر
ب) جمع المعلومات الشخصية

a) Crashing the computer
b) Collecting personal information
c) Installing unsolicited software
d) Redirecting web browsers

ج) تثبيت البرامج غير المرغوب فيها
د) إعادة توجيه مستعرضات الويب.

7) How do Trojans gain access to computers?
a) By being installed via a disk
b) By misleading the user of its true intention
c) By spreading via legitimate email attachments
d) None of the above

7) كيف يمكن لأحصنة طروادة الوصول إلى أجهزة الكمبيوتر؟
أ) بواسطة تثبيتها عبر قرص
ب) بتضليل المستخدم عن نيته الحقيقية
ج) عن طريق الانتشار عبر مرفقات البريد الإلكتروني المشروعة
د) لا شيء مما سبق

8) Which of the following does the lesson NOT list as damage that Trojans can cause?
a) Crashing the computer
b) Deleting files
c) Corrupting data
d) Redirecting web browsers

8) أي مما يلي لا الدرس لا قائمة كما الضرر الذي يمكن أن يسبب حصان طروادة؟
أ) تحطم الكمبيوتر
ب) حذف الملفات
ج) إتلاف البيانات
د) إعادة توجيه مستعرضات الويب

9) " Malware" is the shortened form of _____.
a) Malignant software
b) Malicious software
c) Maleficent software
d) None of the above

9) "البرامج الضارة" هي الصيغة المختصرة لـ_____.
أ) البرمجيات الخبيثة
ب) البرامج الضارة
ج) البرمجيات الخبيثة
د) لا شيء مما سبق

10) الكمبيوتر _____ هو برنامج ضار مستقل يعيد إنتاج نفسه لإصابة أجهزة الكمبيوتر الأخرى.

أ) فيروس
ب) دودة
ج) أ و ب
د) لا شيء مما سبق

10) A computer _____ is an independent malware program that reproduces itself to infect other computers.

a) Virus
b) Worm
c) A and B
d) None of the above

مراجعة الوحدة الثالثة

1) كيف يجذب مجرمو الاحتيال الاحتيالي ضحاياهم؟

أ) من خلال الظهور بمظهر المصدر الشرعي
ب) بتهديدهم
ج) كل من أعلاه
د) لا شيء مما سبق

Module Three: Review Questions

1) How do phishing scam criminals attract their victims?

a) By appearing to be a legitimate source
b) By threatening them
c) Both of the above
d) None of the above

2) ما هي ليست إحدى الطرق التي يستخدم بها التصيد معلومات الأفراد؟

أ) للحصول على معلومات تعريفية مثل رقم الضمان الاجتماعي، لأغراض ضارة

2) What is not one of the ways phishing uses individuals' information?

a) To obtain identifying information such as social security number, for malicious

purposes

b) To commit crimes in the person's name

c) To steal banking details for personal gain

d) To keep the person's information safe

ب) ارتكاب جرائم باسم الشخص

ج) لسرقة التفاصيل المصرفية لتحقيق مكاسب شخصية

د) للحفاظ على معلومات الشخص آمنة

3) What quote is mentioned in the "Identity Theft" lesson?

a) Identity theft is a serious crime that affects millions of Americans each year

b) I don't need to worry about identity theft because no one wants to be me

c) An ounce of prevention is worth a pound of cure

d) If we don't act now to safeguard our privacy, we could all become victims of identity theft

3) ما هو الاقتباس المذكور في درس "سرقة الهوية"؟

أ) سرقة الهوية هي جريمة خطيرة تؤثر على الملايين من الأميركيين كل عام

ب) لا داعي للقلق بشأن سرقة الهوية لأن لا أحد يريد أن يكون أنا

ج) أونصة من الوقاية تساوي رطلا من العلاج

د) إذا لم نتصرف الآن لحماية خصوصيتنا، يمكن أن نصبح جميعا ضحايا لسرقة الهوية

4) Of the following, which is not mentioned in the "Identity Theft" lesson as a way to help prevent identity theft?

a) Be mindful of phishing websites

b) Protect your passwords

c) Utilize an Anti-Virus / Anti-Malware program

d) Don't respond to unsolicited requests for secure information

4) من بين ما يلي، وهو ما لم يرد ذكره في درس "سرقة الهوية" كوسيلة للمساعدة في منع سرقة الهوية؟

أ) يجب أن تضع في اعتبارك مواقع التصيد الاحتيالي

ب) حماية كلمات المرور الخاصة بك

ج) استخدام برنامج مكافحة الفيروسات / مكافحة البرامج الضارة

د) عدم الاستجابة للطلبات غير المرغوب فيها للحصول على معلومات آمنة

5) What is the first thing to do when you discover you have been a victim of cyber bullying?
   a) Respond immediately
   b) Compose yourself before responding
   c) Call the police
   d) Shut down your computer

5) ما هو أول شيء يجب القيام به عندما تكتشف أنك كنت ضحية للتسلط عبر الإنترنت؟
   أ) الاستجابة فورا
   ب) إنشاء نفسك قبل الاستجابة
   ج) اتصل بالشرطة
   د) إيقاف تشغيل الكمبيوتر

6) What is a characteristic of cyber bullying?
   a) Can affect companies as well as individuals
   b) Is limited to adults
   c) Is limited to teenagers
   d) Only affects companies

6) ما هي سمة البلطجة الإلكترونية؟
   أ) يمكن أن تؤثر على الشركات وكذلك الأفراد
   ب) يقتصر على البالغين
   ج) يقتصر على المراهقين
   د) يؤثر فقط على الشركات

7) What does the lesson mention on how cyberstalking is punishable?
   a) Monetary penalties only
   b) Monetary penalties and jail time
   c) Restraining order and monetary penalties
   d) Restraining order and jail time

7) ما الذي يذكره الدرس حول كيفية معاقبة المطاردة الإلكترونية؟
   أ) العقوبات النقدية فقط
   ب) العقوبات النقدية والسجن
   ج) أمر تقييدي وعقوبات مالية
   د) أمر تقييدي والسجن

8) What is not mentioned in the “Cyberstalking” lesson as an anti-stalking tip?
   a) Log out of programs before stepping

8) ما الذي لم يرد ذكره في درس "المطاردة الإلكترونية" كبقشيش لمكافحة المطاردة؟
   أ) تسجيل الخروج من البرامج قبل الابتعاد عن مكتبك
   ب) لا تترك على جهاز الكمبيوتر الخاص بك خلال الليل
   ج) حماية كلمات المرور

away from your desk
b) Do not leave on your computer through the night
c) Protect passwords
d) Keep security software updated

د) تحديث برامج الأمان

9) Receiving an email that says, "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity", is MOST likely characteristic of what?
a) Cyber bullying
b) Cyber stalking
c) Harassment
d) Phishing

9) تلقي رسالة بريد إلكتروني تقول ، "نشك في وجود معاملة غير مصرح بها في حسابك. لضمان عدم اختراق حسابك ، يرجى النقر فوق الرابط أدناه وتأكيد هويتك "، هل من المرجح أن تكون سمة من سمات ماذا؟
أ) التنمر الإلكتروني
ب) المطاردة السيبرانية
ج) التحرش
د) التصيد

10) Cyber _____ can be intentional or unintentional.
a) Bullying
b) Stalking
c) Security breaches
d) Phishing

10) يمكن أن يكون _____ Cyber متعمدًا أو غير مقصود.
أ) التنمر
ب) المطاردة
ج) المخالفات الأمنية
د) التصيد

Module Four: Review Questions

1) You should create a password that is:
   a) Easy for you to remember and easy for others to figure out
   b) Difficult for you to remember but easy for others to figure out
   c) Easy for you to remember but difficult for others to figure out
   d) Difficult for you to remember and difficult for others to figure out

مراجعة الوحدة الرابعة

1) يجب إنشاء كلمة مرور:
   أ) من السهل عليك أن تتذكر وسهلة للآخرين لمعرفة
   ب) من الصعب عليك أن تتذكر ولكن من السهل على الآخرين لمعرفة
   ج) من السهل عليك أن تتذكر ولكن من الصعب على الآخرين لمعرفة
   د) من الصعب عليك أن تتذكر ويصعب على الآخرين معرفة

2) What should your password include?
   a) Upper- and lower-case letters
   b) Upper- and lower-case letters, numbers, and symbols
   c) Numbers and symbols
   d) Upper case letters, numbers, and symbols

2) ما الذي يجب أن تتضمنه كلمة المرور؟
   أ) أحرف الحالة العليا والسفلى
   ب) أحرف الحالة العلوية والسفلية والأرقام والرموز
   ج) الأرقام والرموز
   د) أحرف الحالة العليا والأرقام والرموز

3) What is a denial-of-service attack?
   a) An attack that prevents unintended users from being able to access a network
   b) An attack that prevents users from being able to access a network in the early morning hours only
   c) An attack that prevents users from being able to access a network in the late night hours only
   d) An attack that prevents intended users from being able to access a network

3) ما هو هجوم الحرمان من الخدمة؟
   أ) هجوم يمنع المستخدمين غير المقصودين من الوصول إلى شبكة
   ب) هجوم يمنع المستخدمين من الوصول إلى شبكة في ساعات الصباح الباكر فقط
   ج) هجوم يمنع المستخدمين من الوصول إلى شبكة في ساعات الليل المتأخرة فقط
   د) هجوم يمنع المستخدمين المقصودين من الوصول إلى شبكة

4) Which of the following is not mentioned in the "Denial of Service Attack" lesson as damage that denial of service attacks can cause?
   a) Network performs slowly
   b) A particular website is inaccessible
   c) Receiving a large amount of spam emails
   d) None of the above

4) أي مما يلي لم يرد ذكره في درس "هجوم الحرمان من الخدمة" على أنه ضرر يمكن أن تسببه هجمات الحرمان من الخدمة؟
   أ) شبكة الاتصال ينفذ ببطء
   ب) موقع ويب معين غير قابل للوصول
   ج) تلقي كمية كبيرة من رسائل البريد الإلكتروني غير المرغوب فيها
   د) لا شيء مما سبق

5) What is the purpose of a passive attack?
   a) To find network vulnerabilities and immediately change data
   b) To warn the network user of an impending active attack
   c) To find network vulnerabilities but not change data at the time
   d) To warn the network user of vulnerabilities so the user can fix them

5) ما هو الغرض من الهجوم السلبي؟
   أ) للبحث عن نقاط ضعف الشبكة وتغيير البيانات فورا
   ب) لتحذير مستخدم الشبكة من هجوم نشط وشيك
   ج) للبحث عن نقاط ضعف الشبكة ولكن ليس تغيير البيانات في ذلك الوقت
   د) لتحذير مستخدم الشبكة من الثغرات الأمنية حتى يتمكن المستخدم من إصلاحها

6) In the lesson, passive attacks are likened to:
   a) Eavesdropping
   b) Murder
   c) Downloading
   d) Overloading

6) في الدرس، يتم تشبيه الهجمات السلبية بما يلي:
   أ) تنصت
   ب) قتل
   ج) تحميل
   د) التحميل الزائد

7) What is penetration testing used for?
   a) In a controlled environment, to find vulnerabilities in the network, but not exploit them
   b) In a controlled environment, to find vulnerabilities in the network and exploit those vulnerabilities to see what impact an actual attack would have
   c) In an uncontrolled environment, to find vulnerabilities in the network and exploit those vulnerabilities to see what impact an actual attack would have
   d) In an uncontrolled environment, to find vulnerabilities in the network, but not exploit them

7) ما هو اختبار الاختراق المستخدم؟
   أ) في بيئة خاضعة للرقابة، للعثور على نقاط الضعف في الشبكة، ولكن ليس استغلالها
   ب) في بيئة خاضعة للرقابة، للعثور على نقاط الضعف في الشبكة واستغلال نقاط الضعف هذه لمعرفة ما هو تأثير الهجوم الفعلي سيكون له
   ج) في بيئة غير منضبطة، للعثور على نقاط الضعف في الشبكة واستغلال نقاط الضعف هذه لمعرفة ما هو تأثير الهجوم الفعلي سيكون له
   د) في بيئة غير المنضبط، للعثور على نقاط الضعف في الشبكة، ولكن ليس استغلالها

8) Which of these is discussed in the "Penetration Testing" lesson as a reason that companies implement such testing?
   a) Establish the likelihood of a specific attack occurring
   b) Detect high risk vulnerabilities that can result from a grouping of low-risk vulnerabilities that take place in a

8) أي من هذه التي نوقشت في "اختبار الاختراق" الدرس كسبب أن الشركات تنفيذ مثل هذا الاختبار؟
   أ) تحديد احتمال وقوع هجوم محدد
   ب) اكتشاف نقاط الضعف عالية الخطورة التي يمكن أن تنتج عن مجموعة من نقاط الضعف منخفضة المخاطر التي تحدث في نمط معين
   ج) تحديد تأثير هجوم على شركة

particular pattern

c) Determine the bearing an attack will have on a company

d) All of the above

د) كل ما سبق

9) _____ are orchestrated by individuals or groups to destroy the information systems, networks, etc. of others.

a) Cyber attacks

b) Personal attacks

c) A and B

d) None of the above

9) _____يتم تنسيقها من قبل أفراد أو مجموعات لتدمير أنظمة المعلومات والشبكات وغيرها الخاصة بالآخرين.

أ) الهجمات الإلكترونية

ب) الهجمات الشخصية

ج) أ و ب

د) لا شيء مما سبق

10) Receiving a large amount of spam mail and being locked out of the system after putting in the correct password, but not given access are characteristic of which of the following?

a) Password attack

b) Denial of service

c) Denial of service and password attack

d) None of the above

10) تلقي كمية كبيرة من البريد العشوائي وحظر الدخول إلى النظام بعد إدخال كلمة المرور الصحيحة ، ولكن عدم منح حق الوصول ، هي خصائص أي مما يلي؟

أ) هجوم كلمة المرور

ب) الحرمان من الخدمة

ج) رفض الخدمة وهجوم كلمة المرور

د) لا شيء مما سبق

Module Five: Review Questions

1) What is the best way to store a password?
   a) On a sticky note, on your desk
   b) In your memory
   c) In your phone
   d) In a notebook located in an unlocked desk

مراجعة الوحدة الخامسة

1) ما هي أفضل طريقة لتخزين كلمة المرور؟
   أ) على ملاحظة لاصقة على مكتبك
   ب) في ذاكرتك
   ج) في هاتفك
   د) في دفتر ملاحظات موجود في مكتب غير مقفل

2) When is it best to use one password for all of your accounts?
   a) If you have no more than two accounts
   b) If you have no more than three accounts
   c) Never
   d) If you have no more than four accounts

2) متى يكون من الأفضل استخدام كلمة مرور واحدة لجميع حساباتك؟
   أ) إذا لم يكن لديك أكثر من حسابين
   ب) إذا لم يكن لديك أكثر من ثلاثة حسابات
   ج) أبدا
   د) إذا لم يكن لديك أكثر من أربعة حسابات

3) In the “Two-Step Verification” lesson, which of these is mentioned as something that may be used for authentication purposes?

3) في درس "التحقق بخطوتين"، أي من هذه الخطوات مذكور كشيء يمكن استخدامه لأغراض المصادقة؟
   أ) رمز مميز
   ب) مفتاح

a) Token
b) Key
c) Password
d) All of the above

ج) شعار
د) كل ما سبق

4) The "Two-Step Verification" lesson states that which of these can be used to confirm an individual's identity?
a) Pin
b) Fingerprint
c) Voice recognition
d) All of the above

4) ويشير درس "التحقق من خطوتين" إلى أنه يمكن استخدام أي منها لتأكيد هوية الفرد؟
أ) دبوس
ب) بصمة الإصبع
ج) التعرف على الصوت
د) كل ما سبق

5) What is true of an email attachment with an extension of .doc?
a) It could be a Trojan
b) It should never be downloaded
c) It will always be a legitimate attachment
d) It should only be downloaded if it is sent from a co-worker

5) ما هو صحيح من مرفق البريد الإلكتروني مع تمديدdoc. ؟
أ) يمكن أن يكون طروادة
ب) لا ينبغي أبدا تحميلها
ج) سيكون دائما مرفق شرعي
د) يجب تنزيله فقط إذا تم إرساله من زميل في العمل

6) What is a way to protect yourself when it comes to opening attachments?
a) Regularly update software patches
b) Go with your gut
c) Save and scan the true sender of the attachment
d) All of the above

6) ما هي الطريقة لحماية نفسك عندما يتعلق الأمر بفتح المرفقات؟
أ) تحديث تصحيحات البرامج بانتظام
ب) الذهاب مع أمعائك
ج) حفظ المرسل الحقيقي للمرفق ومسحه ضوئيا
د) كل ما سبق

7) Opening a website that appears to be legitimate but is a spoof can do all of the following, except:
   a) Slow down the speed of your computer
   b) Cause a loss of files
   c) Increase the speed of your computer
   d) Cause a stolen identity

7) فتح موقع ويب يبدو شرعيا ولكنه محاكاة ساخرة يمكن أن يفعل كل ما يلي، باستثناء:
   أ) إبطاء سرعة الكمبيوتر
   ب) تسبب فقدان الملفات
   ج) زيادة سرعة جهاز الكمبيوتر الخاص بك
   د) تسبب في سرقة الهوية

8) Which of these is not mentioned as a precautionary measure to avoid opening a spoof website?
   a) Type the complete URL in the browser
   b) Question the intention of the sender of an unsolicited request to visit a website
   c) Ensure your Anti-Virus / Anti-Spyware is up-to-date
   d) Visit the website from at least two different computers to make sure it is legitimate

8) أي من هذه لم يذكر كإجراء وقائي لتجنب فتح موقع محاكاة ساخرة؟
   أ) اكتب URL الكامل في المستعرض
   ب) السؤال عن نية مرسل طلب غير مطلوب لزيارة موقع ويب
   ج) تأكد من تحديث برنامج مكافحة الفيروسات / مكافحة التجسس
   د) قم بزيارة الموقع من جهازي كمبيوتر مختلفين على الأقل للتأكد من أنه مشروع

9) What can help your organization minimize

9) ما الذي يمكن أن يساعد مؤسستك على تقليل المخاطر؟
   أ) البحث في القانون الاتحادي

risk?

a) Research the federal law
b) Research state laws
c) Having a tool kit of prevention methods
d) None of the above

ب) قوانين الدولة البحث
ج) وجود مجموعة أدوات لطرق الوقاية
د) لا شيء مما سبق

10) One of the easiest steps to keeping your data safe is to craft solid login _____

a) Credentials
b) Identification
c) Name
d) Password

10) واحدة من أسهل الخطوات للحفاظ على أمان بياناتك هي صياغة تسجيل دخول متين_____

أ) أوراق الاعتماد
ب) تحديد الهوية
ج) الاسم
د) كلمة السر

Module Six: Review Questions

1) Credit card numbers:

a) Should only be stored in your phone if you have less than three credit cards
b) Should only be stored in your phone if you have less than two credit cards
c) Should always be stored in your phone
d) Should not be stored in your phone, if possible

مراجعة الوحدة السادسة

1) أرقام بطاقات الائتمان:

أ) يجب تخزينها في هاتفك فقط إذا كان لديك أقل من ثلاث بطاقات ائتمان
ب) يجب تخزينها في هاتفك فقط إذا كان لديك أقل من بطاقتين ائتمانيتين
ج) يجب تخزينها دائما في هاتفك
د) لا ينبغي تخزينها في هاتفك، إذا كان ذلك ممكنا

2) What is a way to safeguard credit card

2) ما هي طريقة حماية معلومات بطاقة الائتمان التي يجب تخزينها

information that you must store on your phone?

a) Encryption
b) Tokenization
c) A and B
d) None of the above

على هاتفك؟

أ) التشفير
ب) الرمز المميز
ج) كل من أعلاه
د) لا شيء مما سبق

3) When setting up a lock on your phone that can be opened with a password:

a) Use a password that is the same as all of your other passwords
b) Use a password that is different from all of your other passwords.
c) Use a password that has no more than five characters
d) Use a password that has no more than three characters

3) عند إعداد قفل على هاتفك يمكن فتحه بكلمة مرور:

أ) استخدام كلمة مرور مماثلة لكافة كلمات المرور الأخرى
ب) استخدم كلمة مرور مختلفة عن جميع كلمات المرور الأخرى.
ج) استخدام كلمة مرور لا تحتوي على أكثر من خمسة أحرف
د) استخدام كلمة مرور لا تحتوي على أكثر من ثلاثة أحرف

4) To create a strong password, it should have:

a) Letters and numbers
b) Numbers and symbols
c) Letters, numbers, and symbols
d) Letters and symbols

4) لإنشاء كلمة مرور قوية، يجب أن يكون:

أ) الحروف والأرقام
ب) الأرقام والرموز
ج) الحروف والأرقام والرموز
د) الحروف والرموز

5) What should be your back-up method if

5) ما هي الطريقة التي يجب أن تكون طريقة النسخة احتياطية إذا

you cannot remember your password?

a) Write down and place in a secure location
b) Save it on your phone
c) Write it down and leave it with a person you trust
d) Any of the above

كنت لا تستطيع تذكر كلمة المرور الخاصة بك؟

أ) دون المكان في مكان آمن
ب) حفظه على هاتفك
ج) اكتبها واتركها مع شخص تثق به
د) أي مما سبق

6) The "Don't Save Passwords" lesson states that passwords should be secured where?

a) In a co-worker's files
b) On the main screen of your phone
c) In a closet
d) In a safe

6) ينص الدرس "عدم حفظ كلمات المرور" على أنه يجب تأمين كلمات المرور أين؟

أ) في ملفات زميل العمل
ب) على الشاشة الرئيسية لهاتفك
ج) في خزانة
د) في خزنة

7) What is the name of the person in the contact list?

a) Bill Johnson
b) John Taylor
c) Jim Smith
d) Bob Jones

7) ما هو اسم الشخص في قائمة جهات الاتصال؟

أ) بيل جونسون
ب) جون تايلور
ج) جيم سميث
د) بوب جونز

8) What was the job title of the person in the contact list?

a) Quality representative
b) Manager

8) ما هو المسمى الوظيفي للشخص في قائمة جهات الاتصال؟

أ) ممثل الجودة
ب) مدير
ج) مدير الحساب
د) ممثل علاقات العملاء

c) Account manager
d) Client relations representative

9) What should you NOT save on your phone?
a) Customers' credit card information
b) Passwords for social media accounts
c) Your boss' birthday
d) The address to a client's office

9) ما الذي لا يجب عليك حفظه على هاتفك؟
أ) معلومات بطاقة ائتمان العملاء
ب) كلمات المرور لحسابات وسائل التواصل الاجتماعي
ج) عيد ميلاد رئيسك في العمل
د) عنوان مكتب العميل

10) How can you protect your phone privacy?
a) Recharge phone every three hours
b) Only use phone after 2:00 p.m.
c) Save passwords on phone
d) Lock phone when not in use

10) كيف يمكنك حماية خصوصية هاتفك؟
أ) إعادة شحن الهاتف كل ثلاث ساعات
ب) استخدم الهاتف فقط بعد الساعة 2:00 مساءً.
ج) حفظ كلمات المرور على الهاتف
د) قفل الهاتف عندما لا يكون قيد الاستخدام

Module Seven: Review Questions

1) What is the MOST effective thing to do if a

مراجعة الوحدة السابعة

1) ما هو الشيء الأكثر فعالية الذي يجب القيام به إذا كان موقع

social media site requires you to put in your address?

a) Put in your actual location
b) Put in a fake address
c) Contact customer service and complain
d) Refuse to open an account

التواصل الاجتماعي يتطلب منك وضع عنوانك؟

أ) ضع موقعك الفعلي
ب) ضع عنوان مزيف
ج) الاتصال بخدمة العملاء والشكوى
د) رفض فتح حساب

2) Which of these is NOT mentioned in the "Don't Reveal Location" lesson of potential things that can happen as a result of inputting your real location?

a) Burglary
b) Harassment
c) Stalking
d) Stolen identity

2) أي من هذه لم يرد ذكره في درس "عدم الكشف عن الموقع" من الأشياء المحتملة التي يمكن أن تحدث نتيجة لإدخال موقعك الحقيقي؟

أ) السطو
ب) تحرش
ج) المطاردة
د) الهوية المسروقة

3) If your birthday is visible on your account, what part of it should you not include?

a) Month
b) Day
c) Year
d) Day of the week you were born

3) إذا كان عيد ميلادك مرئيا على حسابك، فما هو الجزء الذي يجب ألا يتضمنه؟

أ) شهر
ب) يوم
ج) سنة
د) يوم الأسبوع الذي ولدت فيه

4) The first sentence of the "Keep Birthdate Hidden" lesson says, "Giving away your birthday seems like a _____ act..."

a) Harmless
b) Wise
c) Foolish
d) Noble

4) الجملة الأولى من "إبقاء تاريخ الميلاد خفية" الدرس يقول: "التخلي عن عيد ميلادك يبدو وكأنه _____ الفعل"...

أ) غير مؤذي
ب) حكيم
ج) أحمق
د) شريف

5) Which of these is NOT mentioned in “Have Private Profile” as one of the common social media platforms used?
   a) Facebook
   b) YouTube
   c) Instagram
   d) Twitter

5) أي من هذه لم يذكر في "هل الملف الشخصي الخاص" باعتبارها واحدة من منصات وسائل الاعلام الاجتماعية المشتركة المستخدمة؟
   أ) فيسبوك
   ب) يوتيوب
   ج) إنستغرام
   د) التغريد

6) Of the following, which is NOT listed in “Have Private Profile” as a common social media website?
   a) Google+
   b) LinkedIn
   c) Flickr
   d) Pinterest

6) من بين ما يلي وهو غير مدرج في "هل لديك ملف شخصي خاص" كمواقع شائعة على وسائل التواصل الاجتماعي؟
   أ) جوجل بلس
   ب) لينكد إن
   ج) فليكر
   د) بينتيريست

7) You should:
   a) Always link your business and personal accounts
   b) Never link your business and personal accounts
   c) Only link your business and personal accounts if you have only one of each
   d) Only link your business and personal accounts if you have less than three of each

7) يجب عليك:
   أ) ربط دائما عملك والحسابات الشخصية
   ب) لا تربط أبدا بين حساباتك التجارية والشخصية
   ج) ربط فقط عملك والحسابات الشخصية إذا كان لديك واحد فقط من كل
   د) ربط فقط عملك والحسابات الشخصية إذا كان لديك أقل من ثلاثة من كل

8) Which of these is NOT listed as a reason to not link your social media accounts?
   a) Decreased risk of identity theft
   b) Automated posting
   c) Same messages across different platforms
   d) Increased risk of identity theft

8) أي من هذه ليست مدرجة كسبب لعدم ربط حسابات وسائل الاعلام الاجتماعية الخاصة بك؟
   أ) انخفاض خطر سرقة الهوية
   ب) الترحيل التلقائي
   ج) نفس الرسائل عبر منصات مختلفة
   د) زيادة خطر سرقة الهوية

9) This seems like an issue of _____, but many need to be reminded that revealing your location to strangers is never a good idea.
   a) Legal
   b) Common sense
   c) Illegal
   d) None of the above

9) يبدو هذا كأنه قضية _____ ، ولكن يحتاج الكثيرون إلى تذكيرهم بأن الكشف عن موقعك للغرباء ليس فكرة جيدة أبدًا.
   أ) شرعي
   ب) الفطرة السليمة
   ج) غير قانوني
   د) لا شيء مما سبق

10) The Internet is a _____ source.
   a) Private
   b) Public
   c) Personal
   d) Practical

10) الإنترنت مصدر _____.
   أ) خاص
   ب) عامة
   ج) الشخصية
   د) عملي

Module Eight: Review Questions

1) Which of the following are two types of firewalls?
   a) Network and host-based
   b) Anti-Virus and Anti-Spyware
   c) Network and Internet
   d) Host-based and Intranet

مراجعة الوحدة الثامنة

1) أي من التالي نوعين من جدران الحماية؟
   أ) الشبكة والمضيف
   ب) مكافحة الفيروسات ومكافحة التجسس
   ج) شبكة الاتصال والإنترنت
   د) القائمة على المضيف والإنترانت

2) What are firewalls designed to do?
   a) Keep track of but not regulate incoming and outgoing traffic of your network system
   b) Keep track of incoming traffic of your network system
   c) Keep track of and regulate incoming and outgoing traffic of your network system
   d) Keep track of outgoing traffic of your network system

2) ما هي جدران الحماية المصممة للقيام؟
   أ) تتبع ولكن ليس تنظيم حركة المرور الواردة والصادرة من نظام الشبكة
   ب) تتبع حركة المرور الواردة من نظام الشبكة الخاص بك
   ج) تتبع وتنظيم حركة المرور الواردة والصادرة من نظام الشبكة الخاص بك
   د) تتبع حركة المرور الصادرة لنظام الشبكة

3) An example of using a VPN is a company that gives its employees access to its Intranet while not inside of the office. What type of VPN is this?
   a) Site-to-site

3) مثال على استخدام VPN هي شركة تمنح موظفيها حق الوصول إلى إنترانت الخاصة بها بينما لا تكون داخل المكتب. ما نوع الشبكة الافتراضية الخاصة هذا؟
   أ) من موقع إلى موقع
   ب) الوصول عن بعد
   ج) وصول الجمهور

b) Remote access
c) Public access
d) On-site access

د) العمل عن بعد

4) Of the following, which is an actual VPN protocol?
a) Internet Protocol Security
b) Layer 2 Tunneling
c) Point-to-Point Tunneling
d) All of the above

4) من بين ما يلي، ما هو بروتوكول VPN الفعلي؟
أ) أمان بروتوكول الإنترنت
ب) طبقة 2 نفق
ج) نفق من نقطة إلى نقطة
د) كل ما سبق

5) What are threats that Anti-Virus software protects against?
a) Trojans
b) Viruses
c) Browser hijackers
d) All of the above

5) ما هي التهديدات التي يحمي منها برنامج مكافحة الفيروسات؟
أ) احصنه طروادة
ب) فيروسات
ج) متصفح الخاطفين
د) كل ما سبق

6) Which of these companies offers Anti-Virus and Anti-Spyware software?
a) McAfee
b) Norton
c) Kaspersky
d) All of the above

6) أي من هذه الشركات تقدم برامج مكافحة الفيروسات وبرامج مكافحة التجسس؟
أ) مكافي
ب) نورتن
ج) كاسبيرسكي
د) كل ما سبق

7) Which of these is typically the MOST complicated update to install?
   a) High priority
   b) Suggested
   c) Drivers
   d) None of the above

7) أي من هذه عادة التحديث الأكثر تعقيدا لتثبيت؟
   أ) أولوية عالية
   ب) اقترح
   ج) برامج تشغيل
   د) لا شيء مما سبق

8) How often do operating systems release updates?
   a) Regularly
   b) Once every year
   c) Once every two years
   d) Once every three years

8) كم مرة تقوم أنظمة التشغيل بإصدار التحديثات؟
   أ) منتظمة
   ب) مرة كل سنة
   ج) مرة كل سنتين
   د) مرة كل ثلاث سنوات

9) What is a potential danger when using the internet?
   a) Takeover of your computer system
   b) Identity theft
   c) A and B
   d) None of the above

9) ما هو الخطر المحتمل عند استخدام الإنترنت؟
   أ) السيطرة على نظام الكمبيوتر الخاص بك
   ب) سرقة الهوية
   ج) أ و ب
   د) لا شيء مما سبق

10) Firewalls use pre-set security rules to keep track of, and regulate, the incoming and outgoing traffic of your _____.
   a) Social media

10) تستخدم جدران الحماية قواعد أمان محددة مسبقًا لتتبع وتنظيم حركة المرور الواردة والصادرة لـ _____ الخاص بك.
   أ) وسائل التواصل الاجتماعي
   ب) نظام الشبكة
   ج) حسابLinkedIn

b) Network system
c) LinkedIn account
d) Amazon purchases

د) مشتريات أمازون

Module Nine: Review Questions

مراجعة الوحدة التاسعة

1) According to the “Critical Cyber Threats” lesson, which of these is mentioned as a critical infrastructure?
a) Energy
b) Defense
c) Transportation
d) All of the above

1) وفقا لدرس "التهديدات السيبرانية الحرجة"، أي من هذه التهديدات مذكور كبنية تحتية حيوية؟
أ) طاقة
ب) الدفاع
ج) النقل
د) كل ما سبق

2) Which of the following is NOT listed in “Critical Cyber Threats” as a type of critical infrastructure?
a) Food and agriculture
b) Emergency services
c) Communications
d) None of the above

2) أي مما يلي غير مدرج في "التهديدات السيبرانية الحرجة" كنوع من البنية التحتية الحيوية؟
أ) الأغذية والزراعة
ب) خدمات الطوارئ
ج) الاتصالات
د) لا شيء مما سبق

3) In the white supremacist example of Cyber terrorism, what state's ISP was temporarily disabled?
   a) Oregon
   b) Massachusetts
   c) Alabama
   d) New Mexico

3) في المثال العنصري الأبيض للإرهاب الإلكتروني، ما هو برنامج الإنترنت في الولاية الذي تم تعطيله مؤقتا؟
   أ) أوريغون
   ب) ماساتشوستس
   ج) ألاباما
   د) نيو مكسيكو

4) In the Institute for Global Communications Cyber terrorism example, protesters from what country bombarded the institute with thousands of bogus e-mails?
   a) Spain
   b) France
   c) Nigeria
   d) China

4) في مثال معهد الاتصالات العالمية للإرهاب السيبراني قام محتجون من أي بلد بقصف المعهد بآلاف الرسائل الإلكترونية الزائفة؟
   أ) إسبانيا
   ب) فرنسا
   ج) نيجيريا
   د) الصين

5) In the Cyber warfare examples, in 1998, the United States hacked into what country's air defense system?
   a) North Korea
   b) Russia
   c) Serbia
   d) Germany

5) في أمثلة الحرب السيبرانية في عام 1998، اخترقت الولايات المتحدة نظام الدفاع الجوي في أي بلد؟
   أ) كوريا الشمالية
   ب) روسيا
   ج) صربيا
   د) ألمانيا

6) In 2009, a cyber spy network called _____ accessed confidential information belonging to both governmental and private organizations.
   a) GhostNet

6) وفي عام 2009، دخلت شبكة تجسس إلكترونية تسمى _____ إلى معلومات سرية تخص منظمات حكومية وخاصة على حد سواء¬¬¬¬¬.
   أ) شبكة الأشباح
   ب) جاسوس الإنترنت
   ج) شبكة الإنترنت

b) Internet Spy
c) CyberNet
d) Ghost Town

د) مدينة الأشباح

7) In one of the examples in the "Cyber espionage" lesson, an unnamed government official told the Wall Street Journal that cyber spies from which countries had broken into computer systems?
a) Israel and Italy
b) Japan and India
c) Poland and Scotland
d) China and Russia

7) في أحد الأمثلة في درس "التجسس الإلكتروني" قال مسؤول حكومي لم يكشف عن اسمه لصحيفة وول ستريت جورنال إن جواسيس الإنترنت من أي البلدان اقتحموا أنظمة الكمبيوتر؟
أ) إسرائيل وإيطاليا
ب) اليابان والهند
ج) بولندا واسكتلندا
د) الصين وروسيا

8) Canadian researchers revealed in late March that a cyber-spy network based in what country had broken into diplomatic computer systems involving 103 different countries?
a) China
b) Ireland
c) Turkey
d) Iraq

8) كشف باحثون كنديون في أواخر آذار/مارس أن شبكة تجسس إلكتروني مقرها في أي بلد اقتحمت أنظمة كمبيوتر دبلوماسية تضم 103 بلدان مختلفة؟
أ) الصين
ب) أيرلندا
ج) تركيا
د) العراق

9) Critical cyber threats are those that if

9) التهديدات السيبرانية الحرجة هي تلك التي إذا تم تنفيذها ، يمكن

carried out, could have a debilitating effect on an organization, or even _____.

a) A personal account
b) A country
c) A and B
d) None of the above

أن يكون لها تأثير مدمر على المنظمة ، أو حتى._____

أ) حساب شخصي
ب) بلد
ج) أ و ب
د) لا شيء مما سبق

10) _____ are not designed to temporarily disable an organization, but completely destroy it.

a) Viruses
b) Cyber Threats
c) A and B
d) None of the above

10) _____ليست مصممة لتعطيل منظمة بشكل مؤقت ، ولكن تدميرها بالكامل.

أ) الفيروسات
ب) التهديدات السيبرانية
ج) أ و ب
د) لا شيء مما سبق

Module Ten: Review Questions

1) What is cryptography?

a) Secret method of hearing
b) Secret method of speaking
c) Secret method of writing
d) Secret method of seeing

مراجعة الوحدة العاشرة

1) ما هو التشفير؟

أ) طريقة سرية للسمع
ب) طريقة سرية للتحدث
ج) طريقة سرية للكتابة
د) طريقة سرية لرؤية

2) Which of these is NOT an encryption method mentioned in the “Cryptography” lesson?
   a) IDEA
   b) YAR
   c) AES
   d) DES

2) أي من هذه ليست طريقة التشفير المذكورة في "التشفير" الدرس؟
   أ) IDEA
   ب) YAR
   ج) AES
   د) DES

3) The “Digital Forensics” lesson says that who collects and analyzes the data?
   a) Company CEO
   b) Independent forensics specialists
   c) Company employees
   d) Law enforcement

3) "الطب الشرعي الرقمي" الدرس يقول ان من يجمع ويحلل البيانات؟
   أ) الرئيس التنفيذي للشركة
   ب) أخصائيو الطب الشرعي المستقلون
   ج) موظفو الشركة
   د) انفاذ

4) In the Sharon Lopatka example in “Digital Forensics” lesson, who was found to be the person who murdered her?
   a) Robert Glass
   b) Lisa Billingsley
   c) John Smith
   d) Renee Porter

4) في مثال شارون لوباتكا في درس "الطب الشرعي الرقمي"، من وجد أنه الشخص الذي قتلها؟
   أ) روبرت جلاس
   ب) ليزا بيلينجسلي
   ج) جون سميث
   د) رينيه بورتر

5) What is NOT a question that the “Intrusion Detection” lesson states that one must ask before investing in an IDS?
   a) What does our business need in an IDS?

5) ما هو ليس السؤال الذي "كشف التسلل" الدرس تنص على أن المرء يجب أن نسأل قبل الاستثمار في معرفات؟
   أ) ما الذي يحتاجه عملنا فيIDS ؟
   ب) هل يسمح قانون الولاية لأعمالنا بالحصول على معرف؟
   ج) هل يمكننا تحمل تكلفة الحصول على معرف؟

b) Does state law allow our business to have an IDS?
c) Can we afford an IDS?
d) Will our network support the IDS system?

د) هل ستدعم شبكتنا نظامIDS ؟

6) Which of these companies is mentioned as a manufacturer of IDSs?
a) Dakota Alert, Inc.
b) Juniper Networks
c) Linear, LLC
d) All of the above

6) أي من هذه الشركات المذكورة باعتبارها الشركة المصنعة ل IDSs؟
أ) داكوتا تنبيه ، وشركة
ب) جونيبر نتووركز
ج) خطي، ذ.م.م
كل ما سبق

7) The majority of computer hacking crimes are punishable under:
a) Computer Fraud and Abuse Act
b) Civil Rights Act
c) National Security Act
d) Workforce Investment Act

7) يعاقب على معظم جرائم القرصنة الحاسوبية في إطار ما يلي:
أ) قانون الاحتيال وإساءة استخدام الكمبيوتر
ب) قانون الحقوق المدنية
ج) قانون الأمن القومي
د) قانون استثمار القوى العاملة

8) The "Legal Recourse" lesson states there are penalties for committing the following offenses involving computer:
a) Trafficking in Passwords
b) Accessing a Computer to Defraud & Obtain Value
c) Recklessly Damaging by Intentional Access
d) All of the above

8) ينص درس "اللجوء القانوني" على وجود عقوبات على ارتكاب الجرائم التالية التي تنطوي على الكمبيوتر:
أ) الاتجار في كلمات المرور
ب) الوصول إلى كمبيوتر للاحتيال والحصول على قيمة
ج) الإضرار المتهور بالوصول المتعمد
د) كل ما سبق

9) What method of defense can help deter hackers?
   a) VPN
   b) Anti-Virus software
   c) Encryption
   d) Anti-Spyware software

9) ما هي طريقة الدفاع التي يمكن أن تساعد في ردع المتسللين؟
   أ) VPN
   ب) برامج مكافحة الفيروسات
   ج) التشفير
   د) برامج مكافحة برامج التجسس

10) What do intrusion detection systems do?
   a) Notify the intruder that they will be arrested
   b) Notify the company of suspicious activity
   c) Notify the company that an intrusion report has been sent to the federal government
   d) Notify the intruder that the company is aware of their presence and will be fining them

10) ماذا تفعل أنظمة كشف التسلل؟
   أ) إخطار المتسلل بأنه سيتم توقيفه
   ب) إخطار الشركة بالنشاط المشبوه
   ج) إخطار الشركة بإرسال تقرير اقتحام إلى الحكومة الفيدرالية
   د) إخطار المتسلل بأن الشركة على علم بوجودهم وسوف يتم تغريمهم