

تم تحميل هذا الملف من موقع المناهج السعودية



حلول الوحدة الأولى الأمن السيبراني

موقع المناهج ← المناهج السعودية ← الصف الثالث المتوسط ← المهارات الرقمية ← الفصل الأول ← حلول ← الملف

تاريخ إضافة الملف على موقع المناهج: 2024-10-29 09:27:33

ملفات اكتب للمعلم اكتب للطالب الاختبارات الكترونية | اختبارات | حلول | عروض بوربوينت | أوراق عمل
منهج انجليزي | ملخصات وتقارير | مذكرات وبنوك | الامتحان النهائي للمدرس

المزيد من مادة
المهارات
الرقمية:

التواصل الاجتماعي بحسب الصف الثالث المتوسط



صفحة المناهج
السعودية على
فيسبوك

الرياضيات

اللغة الانجليزية

اللغة العربية

التربية الاسلامية

المواد على تلغرام

المزيد من الملفات بحسب الصف الثالث المتوسط والمادة المهارات الرقمية في الفصل الأول

نماذج متنوعة للاختبارات النهائية مع الإجابات عملي

1

أوراق عمل كامل المقرر

2

اختبار منتصف الفصل تحريري

3

اختبار مهارات رقمية نهائي مع الحل

4

اختبار منتصف الفصل تحريري قابل للتعديل

5

الوحدة الأولى : الأمن السيبراني

الدرس الأول : مقدمة في الأمن السيبراني

١. يتعلق مفهوم الأمن السيبراني بالحماية من الوصول غير المصرح به لكل من :

أ. أجهزة الحاسب

ب. الشبكات

ج. البيانات

د. جميع ما سبق

٢. يعبر مصطلح الأمن السيبراني عن جميع الممارسات التي تتم لحماية المعلومات من الوصول غير المصرح به :

أ. صح

ب. خطأ

٣. تزداد أهمية الأمن السيبراني بزيادة أهمية البيانات والمعلومات المتوفرة على الشبكة :

أ. صح

ب. خطأ

٤. كلما قلت أهمية المعلومات كلما كانت عرضة لهجمات القرصنة الحاسوبية :

أ. صح

ب. خطأ

٥. الهدف الأساسي للأمان الإلكتروني هو التركيز على توفير حماية متوازنة للمعلومات والبيانات :

أ. صح

ب. خطأ

٦. عناصر مثلث الحماية CIA :

أ. السرية

ب. التكامل

ج. التوافر

د. جميع ما سبق

٧. من عناصر مثلث الحماية ويقصد بها إتاحة البيانات والمعلومات للأشخاص المعنيين بها فقط والمسموح لهم

بالاطلاع عليها :

أ. السرية

ب. التكامل

ج. التوافر

د. الحماية

٨. من عناصر مثلث الحماية ويشير إلى الحفاظ على دقة وصحة المعلومات :

أ. السرية

ب. التكامل

ج. التوافر

د. الحماية



الوحدة الأولى : الأمن السيبراني

٩. من عناصر مثلث الحماية ويعني ضمان الوصول للمعلومات في الوقت المناسب وبطريقة موثوقة لاستخدامها :

أ. السرية

ب. التكامل

ج. التوافر

د. الحماية

١٠. من أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات :

أ. الحفاظ على سلامة الأجهزة

ب. النسخ الاحتياطي

ج. تحديثات النظام

د. جميع ما سبق

١١. يطلق على استخدام الحاسب كأداة لتحقيق غايات غير قانونية مثل الاحتيال أو سرقة الهويات أو انتهاك

الخصوصية :

أ. التسوق الإلكتروني

ب. المواطنة الرقمية

ج. الجرائم الإلكترونية

د. التعليم عن بعد

١٢. يحدث هذا الاحتيال عندما يتقمص المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية :

أ. الاحتيال الإلكتروني

ب. سرقة الهوية

ج. التسلل الإلكتروني

د. انتهاك الخصوصية

١٣. يحدث هذا الاحتيال عندما يقوم المحتال بانتحال شخصية الضحية واستخدام بياناته لإجراء معاملات مالية أو

أعمال غير قانونية :

أ. الاحتيال الإلكتروني

ب. سرقة الهوية

ج. التسلل الإلكتروني

د. انتهاك الخصوصية

١٤. يحدث هذا الاحتيال عند إصابة أجهزة الحاسب الخاصة بالضحايا ببرامج ضارة يمكنها تسجيل نشاط الحاسب

لمراقبة نشاطاتهم عبر الانترنت :

أ. الاحتيال الإلكتروني

ب. سرقة الهوية

ج. التسلل الإلكتروني

د. انتهاك الخصوصية



الوحدة الأولى : الأمن السيبراني

١٥. يحدث هذا الاحتيال عند محاولة شخص ما التطفل على الحياة الشخصية لشخص آخر :

أ. الاحتيال الإلكتروني

ب. سرقة الهوية

ج. التسلل الإلكتروني

د. انتهاك الخصوصية

١٦. يحدث الاختراق الأمني عند تجاوز طرف غير مصرح به لتدابير الحماية للوصول إلى مناطق محمية من النظام :

أ. صح

ب. خطأ

١٧. يمكن أن يؤدي الاختراق الأمني إلى سيطرة المتسللين على معلومات قيمة والوصول إليها مثل :

أ. حسابات الشركات

ب. الملكية الفكرية

ج. المعلومات الشخصية للعملاء

د. جميع ما سبق

١٨. الهجمة الإلكترونية هي محاولة للوصول غير المصرح به إلى نظام الحوسبة بقصد إحداث ضرر :

أ. صح

ب. خطأ

١٩. في هجوم حجب الخدمات يتم استخدام العديد من أجهزة الحاسب لإغراق موقع ويب مستهدف بحركة المرور :

أ. صح

ب. خطأ

٢٠. هجوم الوسيط نوع من الهجمات الإلكترونية يتطفل فيه المهاجم بين اتصال المستخدم والتطبيق ويجلس في منتصفه متظاهراً بأنه الطرف الآخر :

أ. صح

ب. خطأ

٢١. من الأمثلة على هجوم الوسيط الإلكتروني :

أ. التنصت على الواي فاي

ب. انتحال أسماء النطاقات

ج. التصيد الاحتيالي للبريد الإلكتروني

د. جميع ما سبق

٢٢. تساعد حماية معلوماتك الشخصية في التقليل من خطر سرقة الهوية أو انتحال الشخصية :

أ. صح

ب. خطأ

٢٣. من التدابير التي ينصح باتخاذها للوقاية من الجرائم الإلكترونية :

أ. التحديث الدوري للبرامج

ب. استخدام كلمات المرور القوية

ج. تجنب استخدام شبكات واي فاي العامة

د. جميع ما سبق



الوحدة الأولى : الأمن السيبراني

الدرس الثاني : حماية الحاسب الشخصي

٢٤. يجب حماية أنظمة الحاسب من البرمجيات الضارة :

أ. صح

ب. خطأ

٢٥. تعد الفيروسات إحدى أبرز البرمجيات الضارة وبرامج التجسس التي يتم تثبيتها على جهاز الحاسب دون موافقة المستخدم أو دون معرفته :

أ. صح

ب. خطأ

٢٦. من التغييرات التي قد تكون مؤشراً لإصابة الجهاز بالبرمجيات الضارة :

أ. وجود بطء في أداء جهاز الحاسب

ب. عرض رسائل خطأ متكررة

ج. عرض إعلانات غير مناسبة

د. جميع ما سبق

٢٧. أي مما يلي لا يعد من طرق وقاية أجهزة الحاسب من الإصابة بالبرمجيات الضارة بأنواعها :

أ. تثبيت برنامج مكافحة فيروسات وتحديثه

ب. لا تغيير إعدادات أمان متصفحك

ج. تحميل البرامج من أي موقع

د. استخدام النسخ الاحتياطي للبيانات بانتظام

٢٨. أي مما يلي يعد من طرق وقاية أجهزة الحاسب من الإصابة بالبرمجيات الضارة بأنواعها :

أ. استخدام جدار الحماية

ب. احصل على البرامج من المصدر مباشرة

ج. افحص وحدات التخزين الخارجية قبل استخدامها

د. جميع ما سبق

٢٩. من الخطوات المطلوبة اتخاذها في حالة الاشتباه بوجود برمجيات ضارة على جهاز الحاسب الخاص بك :

أ. التوقف عن التسوق الإلكتروني

ب. تحديث برنامج الحماية

ج. إعادة تعيين المتصفح إلى إعداداته الافتراضية

د. جميع ما سبق

٣٠. هجوم الفدية تم تصميمه لقفل جهاز الحاسب أو منع الوصول إلى ملفاته لابتزاز الضحية بدفع أموال مقابل إلغاء تأمين هذا القفل :

أ. صح

ب. خطأ

٣١. عند استخدام الحاسب يتم تخزين سجل رقمي مفصل للبيانات التي تتم معالجتها أو نقلها على القرص الصلب لجهاز المستخدم فقط :

أ. صح

ب. خطأ



الوحدة الأولى : الأمن السيبراني

٣٢. تفهرس شبكة الانترنت الموقع الإلكتروني ومحتواه اسبوعياً كحد أدنى :

أ. صح

ب. خطأ

٣٣. من البيانات التي يجمعها المتصفح عبر الانترنت :

أ. ملفات تعريف الارتباط

ب. تاريخ التصفح

ج. كلمات المرور المحفوظة

د. جميع ما سبق

٣٤. توفر طريقة للمواقع الإلكترونية للتعرف على المستخدم ومتابعة تفضيلاته :

أ. ملفات تعريف الارتباط

ب. تاريخ التصفح

ج. كلمات المرور المحفوظة

د. عنوان الموقع

٣٥. يتألف من سجل لصفحات الموقع التي قمت بزيارتها في جلسات التصفح السابقة :

أ. ملفات تعريف الارتباط

ب. تاريخ التصفح

ج. كلمات المرور المحفوظة

د. عنوان الموقع

٣٦. عند زيارتك لموقع إلكتروني يتطلب تسجيل الدخول فإن متصفح المواقع الإلكترونية يسأل عما إذا كنت تريد حفظ اسم المستخدم وكلمة المرور :

أ. ملفات تعريف الارتباط

ب. تاريخ التصفح

ج. كلمات المرور المحفوظة

د. عنوان الموقع

٣٧. من الطرق لحماية جهاز الحاسب الشخصي من الهجمات الإلكترونية :

أ. حذف بيانات التصفح

ب. تعطيل النوافذ المنبثقة في المتصفح

ج. تمكين ويندوز ديفندر سمارت سكرين

د. جميع ما سبق

٣٨. تعد مشاركة المعلومات الشخصية مع الآخرين الذين لا تعرفهم شخصياً أحد أكبر المخاطر التي قد تواجهها عبر الانترنت :

أ. صح

ب. خطأ



الوحدة الأولى : الأمن السيبراني

٣٩. من النصائح لتصفح الشبكات الاجتماعية بشكل آمن :

- التحقق من الأشخاص الذين تتواصل معهم
- التحقق من حسابك الخاص
- استخدام كلمات المرور القوية
- جميع ما سبق

٤٠. من غير المهم قراءة سياسة الخصوصية لمنصات الشبكات الاجتماعية التي تشرح بدقة كيفية استخدام المعلومات الخاصة :

- صح
- خطأ

٤١. عند الانضمام إلى شبكة اجتماعية يجب أن تتعرف على كيفية حظر الأعضاء عند الحاجة :

- صح
- خطأ

٤٢. يجب تجنب نشر ما يمكن أن يسيء لوطنك وقيمك وأخلاقك وكبادئك مثل :

- الصور غير اللائقة
- التعليقات العنصرية
- المؤهلات الكاذبة
- جميع ما سبق

2025

2024

