الصف الخامس الابتدائي ٢٠٢٥

بنك اسئلة

المتميز

أ/ محمود سعيد

مراجعة المتميز

تكنولوجيا المعلومات

علي مقررات نوفمبر

أعداد

أ / ياسمين شعيب أ / بيتي صموئيل

ملحق الإجابات بالداخل

نسخة مجانية

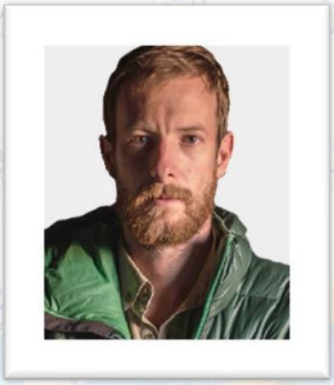
El.Motamyez.School

يمكنكم الحصول على المذكرات والاختبارات من خلال مسح رمز الـ QR Code
أو من خلال صفحة "المتميز - أ/ محمود سعيد".

للإطلاع فقط

الدرس الأول المستكشف النشط

جيف كيربي



عالم بيئة ومصور فوتوغرافي، شارك في بعثات تصوير فوتوغرافي مشوقة في إفريقيا وأمريكا الشمالية، وأكثر ما يصوره هي المناظر الطبيعية والحيوانات.

كيف يستعد جيف كيربي للرحلات؟

يُفكِّر جيدًا في المكان الذي سيتجه إليه، والأشياء التي سيفعلها، وكيف يؤدي عمله بأمان.

الأدوات والمعدات التي يحملها معه جيف أثناء سفره:

-كاميرا خاصة مع العديد من العدسات والبطاريات - جهاز كمبيوتر محمول – طائرة من دون طيار - محركات أقراص صُلْبة خارجية لإنشاء نسخ احتياطية من جميع الصور التي التقطها ويحرص على ذلك في نهاية كل يوم - هاتف محمول لالتقاط صور سريعة لمشاركة أي صور مع زملائه على الفور - أداة تحديد المواقع العالمي (GPS) للتنقل وتحديد الأماكن.

الصور وحقوق النشر

امتلاك الصور	انتهاك حقوق النشر
يعني التمتع بحق قانوني في نشر أو بيع الصور، ويمتلك الجميع حقوق نشر الصور التي يلتقطونها، إلا إذا باعوها قبل أو بعد التقاطها.	يُقصد به استخدام بعض الأشخاص صورًا التقطها آخرون من دون طلب إذنهم، أو من دون شراء حق استخدام الصور.

يمكن للمصورين حماية أعمالهم من انتهاك حقوق النشر عن طريق:

وضع علامة مائية، إضافة معلومات متعلقة بحقوق النشر، مثل: الاسم أو البيانات الوصفية الخاصة بكل صورة.

كيف يضمن جيف كيربي حماية أعماله؟

عن طريق عدم مشاركة صور ذات دقة عالية إلا مع الأشخاص الموثوقين، ويشارك صورًا ذات دقة منخفضة، بحيث لا تبدو جيدة إذا طُبعت أو رفعت على موقع إلكتروني، كما يستخدم البحث من خلال الصور لمعرفة إذا كانت صوره تُستخدم من دون إذنه.

القانون المصري وانتهاك حقوق النشر:

يتعارض انتهاك حقوق النشر مع القانون المصري طبقًا للمادة 69 من الدستور المصري لعام 2014، ولقد صيغت العديد من القوانين المصرية التي تحمي حقوق النشر بناءً على هذه المادة.

الدرس الثـــاني حماية أنفسنا ومعلوماتنا

قراصنة الكمبيوتر: يستخدمون شبكة الإنترنت لاقتحام أنظمة الكمبيوتر لسرقة المعلومات الشخصية.

المعلومات الشخصية: هي معلومات التعريف الشخصي (Personally Identifiable Information) واختصارها PII مثل: اسمك وعنوانك وكلمات المرور الخاصة بك ورقم حسابك البنكي.

يمكن للمخترق استخدام عنوان البريد الإلكتروني وكلمة المرور لأحد الأشخاص لإرسال فيروس لجميع عناوين البريد الإلكتروني الموجودة في بريده الإلكتروني. وكذلك يمكن للمخترق استخدام رقم الحساب المصرفي لأحد البالغين لسرقة أمواله.

طرق الحفاظ على أمان معلومات التعريف الشخصية الخاصة بك

- الحد من المعلومات الشخصية التي تشاركها عبر الإنترنت
- عدم الاشتراك في موقع إلكتروني يطلب منك الكثير من المعلومات الشخصية
- استخدام كلمات مرور قوية تحتوي على أرقام وحروف وعلامات خاصة
- استخدام برامج مكافحة الفيروسات على جميع أجهزتك

- احرص على تحديث أجهزتك وتطبيقاتها بانتظام؛ إذ تتضمن التحديثات تغييرات تحافظ على أمان بياناتك.

الملفات المفقودة: من الضروري أن تتعلم كيفية حماية الملفات التي تنشئها أو تخزنها على الأجهزة من الفيروسات والمشكلات المتعلقة بالبرمجيات وحمايتها من الأخطاء البشرية مثل: سقوط جهاز الكمبيوتر وتحطمه.

طرق حماية الملفات

إنشاء نسخة احتياطية

عن طريق استخدام تطبيقات تنشئ تلقائيًا نسخة احتياطية من ملفاتك.

استخدام جهاز لحفظ الملفات

وتوصيله بجهاز الكمبيوتر مثل: محرك أقراص فلاش أو محرك قرص صُلْب خارجي.

لاحظ: يعد محرك القرص الصلب الخارجي أحد الأجهزة الملحقة التي يمكن استخدامها لحفظ الملفات بشكل آمن وإنشاء نسخ احتياطية، كما يعد القرص الصلب الخارجي أكبر مساحة من ذاكرة الفلاش.

الدرس الثالث
سرية كلمة المرور

يستخدم قراصنة الكمبيوتر العديد من الطرق للحصول على كلمة المرور الخاصة بك، منها:

التصيد الاحتيالي PHISHING
هو إرسال رسالة عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي تبدو حقيقية، ولكنها ليست كذلك.

التصيد الاحتيالي SMISHING
هو نوع آخر من التصيد الاحتيالي يتم بواسطة الرسائل النصية بدلًا من البريد الإلكتروني.

أنواع التصيد الاحتيالي: النوع الأول يخبرك بأنك فزت بجائزة، ولكن عليك أن تعطي تفاصيل حسابك المصرفي لتحصل عليها، النوع الثاني رسالة تحثك على التصرف بسرعة.

لاحظ: عند فتح مرفقات الرسائل الاحتيالية يتم تثبيت برنامج سرقة البيانات على جهاز الكمبيوتر الخاص بالمستخدم، أو يطلب منه إدخال معلومات تعريف شخصية حساسة، مثل: تفاصيل الحساب المصرفي.

يمكنك التعرف على رسائل التصيد الاحتيالي من خلال:

- احتوائها على أخطاء إملائية ونحوية
- احتوائها على طلبات للحصول على بيانات شخصية

لحماية بياناتك الشخصية وأجهزتك من المخترقين تحتاج إلى:

برامج إدارة كلمات المرور

- تنشئ لك كلمات مرور قوية وفريدة لكل حساب من حساباتك.
- تخبرك إذا كانت كلمة المرور لديك ضعيفة جدًّا، أو إذا كانت إحدى كلمات المرور الخاصة بك قد سُرقت عبر الإنترنت.

المصادقة متعددة العوامل

تُستخدم لتعزيز وتقوية كلمة المرور، وتعني تقديم طريقتين على الأقل للتعريف عن نفسك، على أن يجمع بينهم:

- عامل معروف: مثل كلمة المرور أو رقم التعريف الشخصي pin.
- عامل آخر أنت تمتلكه: مثل بريد إلكتروني أو رمز لمرة واحدة.

الدرس الرابع كيفية التعامل مع المواقع الإلكترونية المزيفة

المواقع الالكترونية الاحتيالية : هي المواقع التي تتضمن مواقف مزيفة في محاولة للحصول على بياناتك؛ بهدف التصيد الاحتيالي .

من أمثلة المواقع الاحتيالية

مواقع التسوق عبر الانترنت
لا ترسل إليك أبدا الأغـــراض التي اشتريتها بشكل صحيح .

مواقع برمجيات التخويف
تتضمن تحذيرات مزيفـة تشير إلى وجود مشكلة ما في الكمبيوتر الخاص بك، وأنك في حاجة إلى تحميل تطبيق أو برنامج معين .

مواقع الاحتيال عبر المكافأت
تعرض علـيك جائـزة لا تحصـل عليها مطلقا .

كيفية عمل المواقع الاحتيالية : تعمل المواقع الاحتيالية وفقاً لنفس المبادي حيث :

1- تحاول استدراجك، حيث تسعى إلى إثارة حماسك، أو جذب انتباهك إليها .
2- تحاول اختراق خصوصيتك من خلال: الحصول على معلوماتك الشخصية، أو اختراق جهازك .
3- واخيراً تستغل المعلومات التي توصلت اليها عنك بشكل سيء مثل اختراق جهازك للحصول علي المال .

كيفية تجنب المواقع الإلكترونية الاحتيالية

1- تحقق دائماً من محدد موقع المعلومات URL ، وكذلك تحقق من وجود أخطاء املائية او نحوية لأن المصدر الموثوق سيكون مكتوباً بشكل جيد .
2- اجراء بحث عبر الانترنت لمعرفة ما اذا كان الموقع الذي تستخدمه موقع احتيالي معروف .

ماذا تفعل إذا وقعت ضحية لأحد المواقع الإلكترونية الاحتيالية

1- عليك الإبلاغ عن الأمر، حيث يمكنك أن تخبر شخصا راشدا تثق به مثل : والديك أو معلمك .
2- يمكنك الاتصال بخط مساعدة الطفل، أو بالإدارة العامة لمكافحة جرائم الإنترنت .
3- أبلغ مزود الخدمة، والمتجر الإلكتروني، والبنك الذي تتعامل معه بشأن هذا الموقع الاحتيالي، بمساعدة معلمك أو أحد أفراد أسرتك .

تتألف محددات مواقع المعلومات أو موقع الويب (URL) من ثلاث أجزاء رئيسية هي :

1- **البروتوكول :** يبدأ به محدد موقع المعلومات ويحدد كيفية نقل المعلومات ومن أمثلته (HTTP – HTTPS)
2- **اسم المورد :** هو خادم الشبكة او الموقع الالكتروني المطلوب ويوضح من يملك هذا الموقع وينتهي بـ .COM ، .NET ، ORG.
3- **مسار الملف :** يمثل الجزء الأخير من الـــ URL ويحدد اسم المورد الذي يمنح الرابط الالكتروني إمكانية الوصول اليه .

بنك أسئلة المتميز على مقررات شهر نوفمبر

تشمل اسئلة الوزارة واختبارات المحافظات

السؤال الأول: اختر الإجابة الصحيحة

١ يجب ابلاغ ..... الذي تتعامل معه اذا تمت سرقة حسابك المصرفي .
أ المعلم ب البنك ج صديقك

٢ المصادقة متعددة العوامل هي تقديم ..... على الأقل لتعريف المستخدم عن نفسه .
أ طريقة ب طريقتين ج ثلاث طرق

٣ ..... يستخدمون شبكة الإنترنت لاقتحام أنظمة الكمبيوتر لسرقة المعلومات الشخصية .
أ قراصنة الكمبيوتر ب المبرمجون ج مدخلي البيانات

٤ إذا وصلتك رسالة تطلب منك الحصول على الكثير من البيانات الشخصية، فهذه إحدى رسائل .....
أ البنك ب التصيد الاحتيالي PHISHING ج المصادقة متعددة العوامل

٥ يعد ..... أحد الأجهزة الملحقة التى تستخدم لحفظ الملفات بشكل أمن.
أ القرص الصلب الخارجي ب لوحة المفاتيح ج الفأرة

٦ ..... هو المفهوم نفسه للتصيد الاحتيالي، لكنه يتم بواسطة الرسائل النصية بدلًا من البريد الإلكتروني .
أ التصيد الاحتيالي PHISHING ب الفيروسات ج التصيد الاحتيالي SMISHING

٧ تستخدم ذاكرة الفلاش في .....
أ طباعة الملفات ب عمل نسخه احتياطية لملفاتك ج حذف الملفات

٨ لتحافظ على أمان بياناتك استخدم برامج ..... على جميع أجهزتك
أ الوسائط ب مكافحة الفيروسات ج تعديل الصور

٩ يمكن للمخترق إرسال فيروس إلى جميع عناوين البريد الإلكتروني الموجودة فى بريدك الإلكتروني إذا تمكن من معرفة .....
أ رقم حسابك المصرفى ب عنوان بريدك الإلكتروني وكلمة المرور ج تاريخ ميلادك

١٠ مواقع ..... التي تتضمن تحذيرات مزيفة، وأنك في حاجة إلى تحميل تطبيق أو برنامج معين.
أ التسوق ب برمجيات التخويف ج الموسوعات

١١ لتجنب المواقع الاحتيالية الإلكترونية عليك التحقق من عدم وجود.....
أ أخطاء إملائية ب دقة إملائية ج محتوى موثوق

١٢ يستخدم ..... لمشاركة المعلومات عبر شبكة مغلقة، وهو أكثر أمانًا
أ الإنترنت ب الإنترانت ج الويب

١٣ يمثل الجزء الأخير من الـ URL .....
أ المورد ب البروتوكول (Protocol) ج مسار الملف

١٤ لعمل فرز أو ترتيب للخلايا نذهب الي تبويب .....
أ ادراج INSERT ب عرض VIEW ج بيانات DATA

١٥ يجب أن تكون كلمات المرور ..... لكل موقع إلكتروني تسجل فيه.
أ متشابهة ب متكررة ج مختلفة

١٦ لتخزين المعلومات ومشاركتها نستخدم .....
أ الماسح الضوئي ب الطابعة ج ذاكرة فلاش

١٧ ..... هو إرسال رسالة عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي تبدو حقيقية، ولكنها ليست كذلك .
أ التصيد الاحتيالي PHISHING ب الفيروسات ج التصيد الاحتيالي SMISHING

١٨ يبدأ محدد موقع المعلومات (URL) بـ .....
أ المورد ب البروتوكول (Protocol) ج مسار الملف

١٩ عند فتح مرفقات الرسالة الاحتيالية يتم ..... برنامج سرقة البيانات على جهاز الكمبيوتر الخاص بالمستخدم .
أ حذف ب تحديث ج تثبيت

٢٠ ..... تتمثل في اسمك وعنوانك وتاريخ ميلادك وكلمات المرور الخاصة بك.
أ المعلومات العامة ب معلومات التعريف الشخصي ج معلومات الإنترنت

٢١ ينشئ لك برنامج إدارة كلمات المرور كلمات مرور .....
أ قوية ب ضعيفة ج متكررة

٢٢ احرص على ..... أجهزتك وتطبيقاتها بانتظام للحفاظ على أمان معلوماتك الخاصة.
أ تحديث ب إغلاق ج إعادة تثبيت

٢٣ مواقع ..... تعرض عليك جائزة لا تحصل عليها مطلقًا.
أ التخويف ب الاحتيال عبر المكافأة ج التسوق

٢٤ يساعد ..... على إدارة الملفات باستخدام تكنولوجيا المعلومات
أ إنشاء مجلدات ب حذف المجلدات ج نسخ المجلدات

٢٥ كل الطرق التالية تمكنك من الحفاظ على أمان معلوماتك الشخصية ما عدا.....
أ استخدام كلمات مرور قوية ب استخدام مكافح الفيروسات. ج مشاركة اسمك، وعنوانك مع جميع المواقع

٢٦ يمكنك التحقق من المواقع الإلكترونية عن طريق .....وهو عنوان الموقع الإلكتروني.

أ الحقائق ب محدد موقع المعلومات URL ج المدونات الرقمية

٢٧ .....يوضح مَنْ يملك هذا الموقع .

المورد البروتوكول (Protocol) مسار الملف

٢٨ SMISHING هو نفس مصطلح التصيد الاحتيالي ولكنه مرسل من قبل.....

أ بريد إلكتروني ب رسالة نصية ج فيسبوك

٢٩ يمكن ..... أن يقوم باستخدام رقم الحساب المصرفي لأحد البالغين لسرقة أمواله .

أ للمخترق ب لموظف البنك ج لصديقك

٣٠ تعمل المواقع الإلكترونية الاحتيالية للحصول على .....

أ جهاز الكمبيوتر الخاص بك ب محدد موقع المعلومات URL ج معلوماتك الشخصية

السؤال الثاني

ضع علامة (√) أمام العبارة الصحيحة وعلامة (×) أمام العبارة غير الصحيحة

١ يستخدم قراصنة الكمبيوتر معلوماتك الشخصية مثل أسمك وعنوانك وتاريخ ميلادك لاقتحام الكمبيوتر الخاص بك. ( )

٢ تستخدم المصادقة متعددة العوامل لتعزيز وتقوية كلمات المرور. ( )

٣ يعد حدوث الأعطال للأجهزة الإلكترونية أمرً ا مستبعدا. ( )

٤ يخبرك برنامج إدارة كلمات المرور إذا كانت كلمات المرور التي لديك ضعيفة أو استخدمتها من قبل. ( )

٥ يمكننا التقاط الصور الفوتوغرافية بواسطة الماسح الضوئي ( )

٦ عند فتح مرفقات رسالة التصيد الاحتيالي قد يطلب منك إدخال معلومات شخصية. ( )

٧ التصيد الاحتيالي يمكن من خلال البريد الإلكتروني ولا يمكن من خلال الرسائل النصية . ( )

٨ التصيد الاحتيالي phishing هو الاحتيال عبر الرسائل النصية ( )

٩ أحد الطرق للحفاظ على أمان معلومات التعريف الشخصية الخاصة بك هو الحد من المعلومات الشخصية التى تشاركها عبر الانترنت . ( )

١٠ بعض التطبيقات والبرمجيات تنشئ تلقائيًا نسخا احتياطية من الملفات للحفاظ عليها. ( )

١١ يفضل الاشتراك فى المواقع الإلكترونية التى تطلب منك الكثير من المعلومات الشخصية . ( )

١٢ من الضروري لأمان بياناتك استخدام كلمات مرور قوية تحتوي على حروف وأرقام وعلامات. ( )

١٣ يجب استخدام كلمات مرور ضعيفة للحفاظ على أمان معلومات التعريف الشخصي الخاص بك. ( )

١٤ يمكن للمخترق إرسال فيروس إلى جميع عناوين البريد الإلكتروني المسجلة لديك. ( )

١٥ للحفاظ على أمان معلوماتك عليك الحد من مشاركة المعلومات الشخصية عبر الإنترنت. ( )

١٦ جميع المواقع الاحتيالية تعمل وفقا للمبادئ نفسها مثل الاستدراج والحصول على المعلومات الشخصية . ( )

١٧ اكتشاف المخترق لكلمة مرورك لا يمثل أي تهديد على بياناتك. ( )

١٨ يجب عمل نسخ احتياطية من الملفات المهمة منعا لاحتمالية فقدانها على جهازك. ( )

١٩ للحفاظ على أمان معلومات التعريف الشخصية الخاصة بك حدث أجهزتك بانتظام. ( )

٢٠ الاختراق هو استخدام عنوان بريدك الإلكتروني وكلمة المرور لإرسال فيروس إلى جميع عناوين البريد الإلكتروني الموجودة فى بريدك الالكتروني . ( )

٢١ نستخدم ذاكرة الفلاش لحفظ الملفات الكبيرة ( )

٢٢ لا يفضل أن تخبر شخصا راشدا تثق به إذا وقعت ضحية للمواقع الاحتيالية. ( )

٢٣ من أشكال التصيد الاحتيالي رسالة تخبرك بأنك فزت بجائزة، لكن عليك أن تعطي تفاصيل رقم حسابك المصرفي (البنكي) لتحصل عليها. ( )

٢٤ من المواقع الموثوقة مواقع التسوق عبر الإنترنت التي لا ترسل إليك الأغراض التي اشتريتها بشكل صحيح ( )

٢٥ البروتوكول هو خادم الشبكة أو الموقع الإلكتروني، وغالبًا ما ينتهي بـــ .COM ( )

٢٦ تنشىء بعض التطبيقات والبرمجيات تلقائيا نسخا إحتياطيا من الملفات. ( )

٢٧ تضمن المصادقة متعددة العوامل وصول أي شخص إلى حساباتك الإلكترونية. ( )

٢٨ تستغل المواقع الاحتيالية المعلومات التي توصلت إليها عنك بشكل سيئ للحصول علي المال . ( )

٢٩ التصيد الاحتيالي هو إرسال رسالة بريد إلكتروني تبدو حقيقة ولكنها ليست كذلك . ( )

٣٠ ليس من الضروري أن تتعلم كيفية حماية الملفات التي تنشئها أو تخزنها. ( )

٣١ يمكن لقراصنة الكمبيوتر الحصول على كلمة المرور الخاصة بك بطريقة واحدة فقط ( )

٣٢ من أنواع التصيد الاحتيالي نوع يحثك على التصرف بسرعة. ( )

٣٣ ليس من الضروري إنشاء كلمات مرور قوية لحماية بياناتك الشخصية من المخترقين . ( )

٣٤ ليس من الضروري إبلاغ البنك الذي تتعامل معه بشأن أي موقع احتيالي. ( )

٣٥ نستخدم الكاميرا الرقمية لنقل الملفات ومشاركتها. ( )

٣٦ لا يمكن التعرف على رسائل التصيد الاحتيالي. ( )

٣٧ يمكن استخدام قرص صلب خارجي لعمل نسخة احتياطية من ملفاتك وحفظها. ( )

٣٨ مصدر المعلومات الموثوق يكون مكتوبًا جيدا مع عدم وجود أخطاء إملائية . ( )

٣٩ لتجنب المواقع الاحتيالية، عليك عدم التحقق من محدد موقع المعلومات URL . ( )

٤٠ ليس من الضروري أن تتوخى الحذر عند زيارة مواقع إلكترونية جديدة. ( )

٤١ يجب عليك الاشتراك في أي موقع إلكتروني يطلب منك الكثير من المعلومات الشخصية. ( )

انتهت الأسئلة مع أطيب الامنيات بالنجاح والتوفيق

الصف الخامس الابتدائي ٢٠٢٥

بنك اسئلة

المتميز

أ/ محمود سعيد

الاجابات النموذجية لبنك الاسئلة

تكنولوجيا المعلومات

علي مقررات نوفمبر

5 الصف الخامس

أعداد

أ / ياسمين شعيب أ / بيتي صموئيل

بنك أسئلة المتميز على مقررات شهر نوفمبر

تشمل اسئلة الوزارة واختبارات المحافظات

السؤال الأول: اختر الإجابة الصحيحة

١ يجب ابلاغ ..... الذي تتعامل معه اذا تمت سرقة حسابك المصرفي .
أ المعلم ب البنك ج صديقك

٢ المصادقة متعددة العوامل هي تقديم ..... على الأقل لتعريف المستخدم عن نفسه .
أ طريقة ب طريقتين ج ثلاث طرق

٣ ..... يستخدمون شبكة الإنترنت لاقتحام أنظمة الكمبيوتر لسرقة المعلومات الشخصية .
أ قراصنة الكمبيوتر ب المبرمجون ج مدخلي البيانات

٤ إذا وصلتك رسالة تطلب منك الحصول على الكثير من البيانات الشخصية، فهذه إحدى رسائل .....
أ البنك ب التصيد الاحتيالي PHISHING ج المصادقة متعددة العوامل

٥ يعد ..... أحد الأجهزة الملحقة التى تستخدم لحفظ الملفات بشكل أمن.
أ القرص الصلب الخارجي ب لوحة المفاتيح ج الفأرة

٦ ..... هو المفهوم نفسه للتصيد الاحتيالي، لكنه يتم بواسطة الرسائل النصية بدلًا من البريد الإلكتروني .
أ التصيد الاحتيالي PHISHING ب الفيروسات ج التصيد الاحتيالي SMISHING

٧ تستخدم ذاكرة الفلاش في .....
أ طباعة الملفات ب عمل نسخه احتياطية لملفاتك ج حذف الملفات

٨ لتحافظ على أمان بياناتك استخدم برامج ..... على جميع أجهزتك
أ الوسائط ب مكافحة الفيروسات ج تعديل الصور

٩ يمكن للمخترق إرسال فيروس إلى جميع عناوين البريد الإلكتروني الموجودة فى بريدك الإلكتروني إذا تمكن من معرفة .....
أ رقم حسابك المصرفى ب عنوان بريدك الإلكتروني وكلمة المرور ج تاريخ ميلادك

١٠ مواقع ..... التي تتضمن تحذيرات مزيفة، وأنك في حاجة إلى تحميل تطبيق أو برنامج معين.
أ التسوق ب برمجيات التخويف ج الموسوعات

١١ لتجنب المواقع الاحتيالية الإلكترونية عليك التحقق من عدم وجود.....
أ أخطاء إملائية ب دقة إملائية ج محتوى موثوق

١٢ يستخدم ..... لمشاركة المعلومات عبر شبكة مغلقة، وهو أكثر أمانًا
أ الإنترنت ب الإنترانت ج الويب

١٣ يمثل الجزء الأخير من الـ URL .....
أ المورد ب البروتوكول (Protocol) ج مسار الملف

١٤ لعمل فرز أو ترتيب للخلايا نذهب الي تبويب .....
أ ادراج INSERT ب عرض VIEW ج بيانات DATA

١٥ يجب أن تكون كلمات المرور ..... لكل موقع إلكتروني تسجل فيه.
أ متشابهة ب متكررة ج مختلفة

١٦ لتخزين المعلومات ومشاركتها نستخدم .....
أ الماسح الضوئي ب الطابعة ج ذاكرة فلاش

١٧ ..... هو إرسال رسالة عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي تبدو حقيقية، ولكنها ليست كذلك .
أ التصيد الاحتيالي PHISHING ب الفيروسات ج التصيد الاحتيالي SMISHING

١٨ يبدأ محدد موقع المعلومات (URL) بـ .....
أ المورد ب البروتوكول (Protocol) ج مسار الملف

١٩ عند فتح مرفقات الرسالة الاحتيالية يتم ..... برنامج سرقة البيانات على جهاز الكمبيوتر الخاص بالمستخدم .
أ حذف ب تحديث ج تثبيت

٢٠ ..... تتمثل في اسمك وعنوانك وتاريخ ميلادك وكلمات المرور الخاصة بك.
أ المعلومات العامة ب معلومات التعريف الشخصي ج معلومات الإنترنت

٢١ ينشئ لك برنامج إدارة كلمات المرور كلمات مرور .....
أ قوية ب ضعيفة ج متكررة

٢٢ احرص على ..... أجهزتك وتطبيقاتها بانتظام للحفاظ على أمان معلوماتك الخاصة.
أ تحديث ب إغلاق ج إعادة تثبيت

٢٣ مواقع ..... تعرض عليك جائزة لا تحصل عليها مطلقًا.
أ التخويف ب الاحتيال عبر المكافأة ج التسوق

٢٤ يساعد ..... على إدارة الملفات باستخدام تكنولوجيا المعلومات
أ إنشاء مجلدات ب حذف المجلدات ج نسخ المجلدات

٢٥ كل الطرق التالية تمكنك من الحفاظ على أمان معلوماتك الشخصية ما عدا.....
أ استخدام كلمات مرور قوية ب استخدام مكافح الفيروسات. ج مشاركة اسمك، وعنوانك مع جميع المواقع

٢٦ يمكنك التحقق من المواقع الإلكترونية عن طريق .....وهو عنوان الموقع الإلكتروني.
أ الحقائق ب محدد موقع المعلومات URL ج المدونات الرقمية

٢٧ .....يوضح مَنْ يملك هذا الموقع .
المورد البروتوكول (Protocol) مسار الملف

٢٨ SMISHING هو نفس مصطلح التصيد الاحتيالي ولكنه مرسل من قبل.....
أ بريد إلكتروني ب رسالة نصية ج فيسبوك

٢٩ يمكن ..... أن يقوم باستخدام رقم الحساب المصرفي لأحد البالغين لسرقة أمواله .
أ للمخترق ب لموظف البنك ج لصديقك

٣٠ تعمل المواقع الإلكترونية الاحتيالية للحصول على .....
أ جهاز الكمبيوتر الخاص بك ب محدد موقع المعلومات URL ج معلوماتك الشخصية

السؤال الثاني
ضع علامة (√) أمام العبارة الصحيحة وعلامة (×) أمام العباراة غير الصحيحة

١ يستخدم قراصنة الكمبيوتر معلوماتك الشخصية مثل أسمك وعنوانك وتاريخ ميلادك لاقتحام الكمبيوتر الخاص بك. √
٢ تستخدم المصادقة متعددة العوامل لتعزيز وتقوية كلمات المرور. √
٣ يعد حدوث الأعطال للأجهزة الإلكترونية أمرً ا مستبعدا. ×
٤ يخبرك برنامج إدارة كلمات المرور إذا كانت كلمات المرور التي لديك ضعيفة أو استخدمتها من قبل. √
٥ يمكننا التقاط الصور الفوتوغرافية بواسطة الماسح الضوئي ×
٦ عند فتح مرفقات رسالة التصيد الاحتيالي قد يطلب منك إدخال معلومات شخصية. √
٧ التصيد الاحتيالي يمكن من خلال البريد الإلكتروني ولا يمكن من خلال الرسائل النصية . ×
٨ التصيد الاحتيالي phishing هو الاحتيال عبر الرسائل النصية ×
٩ أحد الطرق للحفاظ على أمان معلومات التعريف الشخصية الخاصة بك هو الحد من المعلومات الشخصية التى تشاركها عبر الانترنت . √
١٠ بعض التطبيقات والبرمجيات تنشئ تلقائيًا نسخا احتياطية من الملفات للحفاظ عليها. √
١١ يفضل الاشتراك فى المواقع الإلكترونية التى تطلب منك الكثير من المعلومات الشخصية . ×
١٢ من الضروري لأمان بياناتك استخدام كلمات مرور قوية تحتوي على حروف وأرقام وعلامات. √
١٣ يجب استخدام كلمات مرور ضعيفة للحفاظ على أمان معلومات التعريف الشخصي الخاص بك. ×

١٤ يمكن للمخترق إرسال فيروس إلى جميع عناوين البريد الإلكتروني المسجلة لديك. ✓
١٥ للحفاظ على أمان معلوماتك عليك الحد من مشاركة المعلومات الشخصية عبر الإنترنت. ✓
١٦ جميع المواقع الاحتيالية تعمل وفقا للمبادئ نفسها مثل الاستدراج والحصول على المعلومات الشخصية . ✓
١٧ اكتشاف المخترق لكلمة مرورك لا يمثل أي تهديد على بياناتك. ✗
١٨ يجب عمل نسخ احتياطية من الملفات المهمة منعا لاحتمالية فقدانها على جهازك. ✓
١٩ للحفاظ على أمان معلومات التعريف الشخصية الخاصة بك حدث أجهزتك بانتظام. ✓
٢٠ الاختراق هو استخدام عنوان بريدك الإلكتروني وكلمة المرور لإرسال فيروس إلى جميع عناوين البريد الإلكتروني الموجودة فى بريدك الالكتروني . ✓
٢١ نستخدم ذاكرة الفلاش لحفظ الملفات الكبيرة ✗
٢٢ لا يفضل أن تخبر شخصا راشدا تثق به إذا وقعت ضحية للمواقع الاحتيالية. ✗
٢٣ من أشكال التصيد الاحتيالي رسالة تخبرك بأنك فزت بجائزة، لكن عليك أن تعطي تفاصيل رقم حسابك المصرفي (البنكي) لتحصل عليها. ✓
٢٤ من المواقع الموثوقة مواقع التسوق عبر الإنترنت التي لا ترسل إليك الأغراض التي اشتريتها بشكل صحيح ✗
٢٥ البروتوكول هو خادم الشبكة أو الموقع الإلكتروني، وغالبًا ما ينتهي بـــ .COM ✗
٢٦ تنشىء بعض التطبيقات والبرمجيات تلقائيا نسخا إحتياطيا من الملفات. ✓
٢٧ تضمن المصادقة متعددة العوامل وصول أي شخص إلى حساباتك الإلكترونية. ✗
٢٨ تستغل المواقع الاحتيالية المعلومات التي توصلت إليها عنك بشكل سيئ للحصول علي المال . ✓
٢٩ التصيد الاحتيالي هو إرسال رسالة بريد إلكتروني تبدو حقيقة ولكنها ليست كذلك . ✓
٣٠ ليس من الضروري أن تتعلم كيفية حماية الملفات التي تنشئها أو تخزنها. ✗
٣١ يمكن لقراصنة الكمبيوتر الحصول على كلمة المرور الخاصة بك بطريقة واحدة فقط ✗
٣٢ من أنواع التصيد الاحتيالي نوع يحثك على التصرف بسرعة. ✓
٣٣ ليس من الضروري إنشاء كلمات مرور قوية لحماية بياناتك الشخصية من المخترقين . ✗
٣٤ ليس من الضروري إبلاغ البنك الذي تتعامل معه بشأن أي موقع احتيالي. ✗
٣٥ نستخدم الكاميرا الرقمية لنقل الملفات ومشاركتها. ✗
٣٦ لا يمكن التعرف على رسائل التصيد الاحتيالي. ✗
٣٧ يمكن استخدام قرص صلب خارجى لعمل نسخة احتياطية من ملفاتك وحفظها. ✓
٣٨ مصدر المعلومات الموثوق يكون مكتوبًا جيدا مع عدم وجود أخطاء إملائية . ✓

٣٩ لتجنب المواقع الاحتيالية، عليك عدم التحقق من محدد موقع المعلومات URL . ✗

٤٠ ليس من الضروري أن تتوخى الحذر عند زيارة مواقع إلكترونية جديدة. ✗

٤١ يجب عليك الاشتراك في أي موقع إلكتروني يطلب منك الكثير من المعلومات الشخصية. ✗

انتهت الأسئلة مع أطيب الامنيات بالنجاح والتوفيق