CyberEco

معًا لدعم السلامة الرقمية

Together to support digital safety

التّزوير والاحتيال عبر الإنترنت

شرائح العَرْض

حَقِيبَة خاصَّة بالمُدَرِّب

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

المرحلة الإعداديّة

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa
00974 404 663 78
00974 404 663 62

فِهْرس المُحتَوى العِلْميّ

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تمهيد	5 دقائق
الجُزْء النَّظريّ من المادَّة	25 دقيقة
عَرْض الفيديوهات التَّعليميَّة	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الأَلْعَاب التَّدريبيَّة	25 دقيقة
حِوَار ونِقَاش مع الطَّلَبة	15 دقيقة
مَشروع التَّخرُّج	5 دقائق
المُدَّة الزَّمنيَّة للورشَة	ساعتان

الفَصْل الأَوَّل
مفهوم التَّزوير والاحتيال عبر الإنترنت وأنواعه

أوَّلًا

مفهوم الاحتيال عبر الإنترنت

الاحتيال عبر الإنترنت

نوع من أنواع الخِداع والحيل التي تتمّ عبر شبكة الإنترنت، وغالبًا ما تَحدُث هذه الجرائم في غرف الدَّردشة أو عبر البريد الإلكترونيّ أو على المنتديات أو مواقع الإنترنت (الويب)، والهدف من هذه الجرائم هو الاحتيال على العملاء والمُستخدِمين عن طريق سرقة الأموال والمعلومات الشَّخصيَّة المهمَّة، وغيرها من الأغراض الأخرى.

الاحتيال المعلوماتيّ

من المفاهيم المُرْتَبِطَة بمفهوم الاحتيال عبر الإنترنت، ويُقْصَد به: الخِداع أو الغِشّ المعلوماتيّ الذي يقوم على التَّلاعب في نُظُم المُعالَجة الآليَّة للمعلومات، بغرض الحصول -دون وجه حَقّ- على خدمات أو أموال أو أصول معيَّنة.

الاحتيال أو النصب عبر الإنترنت

الاستيلاء على مال الآخرين بوسيلةٍ يَشُوبها الخِداع، ما يتسبَّب في تَسَلُّم هذا المال عن طريق أجهزة الحاسوب.

ثانيًا: أسباب الوقوع ضحيَّةً للاحتيال عَبْر الإنترنت

1. قلَّة وَعْي الأفراد بكيفيَّة استخدام وسائل التَّواصُل الاجتماعيّ.
2. الاستخدام الخاطئ لمواقع الإنترنت والدُّخول إلى مواقع إلكترونيَّة غير آمِنَة.
3. نَشْر معلومات شخصيَّة على مواقع التَّواصُل الاجتماعيّ.
4. ضَعْف الأنظمة الإلكترونيَّة للمؤسَّسات والشَّركات.
5. المَتاجِر الإلكترونيَّة المُزيَّفة التي تُؤدِّي إلى خسارة الأموال.
6. انتشار منصَّات تبادل العملات الرَّقميَّة.
7. سرقة معلومات حسَّاسة عن الأفراد من الشَّركات والمؤسَّسات دون عِلْم إدارات الشركات.

ثالثًا

أنواع وأشكال الاحتيال عبر الإنترنت

البريد الإلكترونيّ

من طُرق الاحتيال عبر الإنترنت التي تُعَدّ الأكثر خِداعًا ومَكْرًا، إرسال بريد إلكترونيّ مُزوَّر يبدو كأنَّه أُرسِل من صديق أو من جِهة رسميَّة، في حين أنَّها لَيْسَت سوى عمليَّة تَصَيُّدٍ عبر الإنترنت.

الهاتف الذّكيّ

يتسبّب تثبيت تطبيقات مُقَرْصَنة (مُهَكّرة) أو مجهولة المصدر، وكذلك الضّغط على روابط مجهولة المصدر، في اختراق البيانات الشّخصيّة كالصّور والملفّات.

الحاسوب

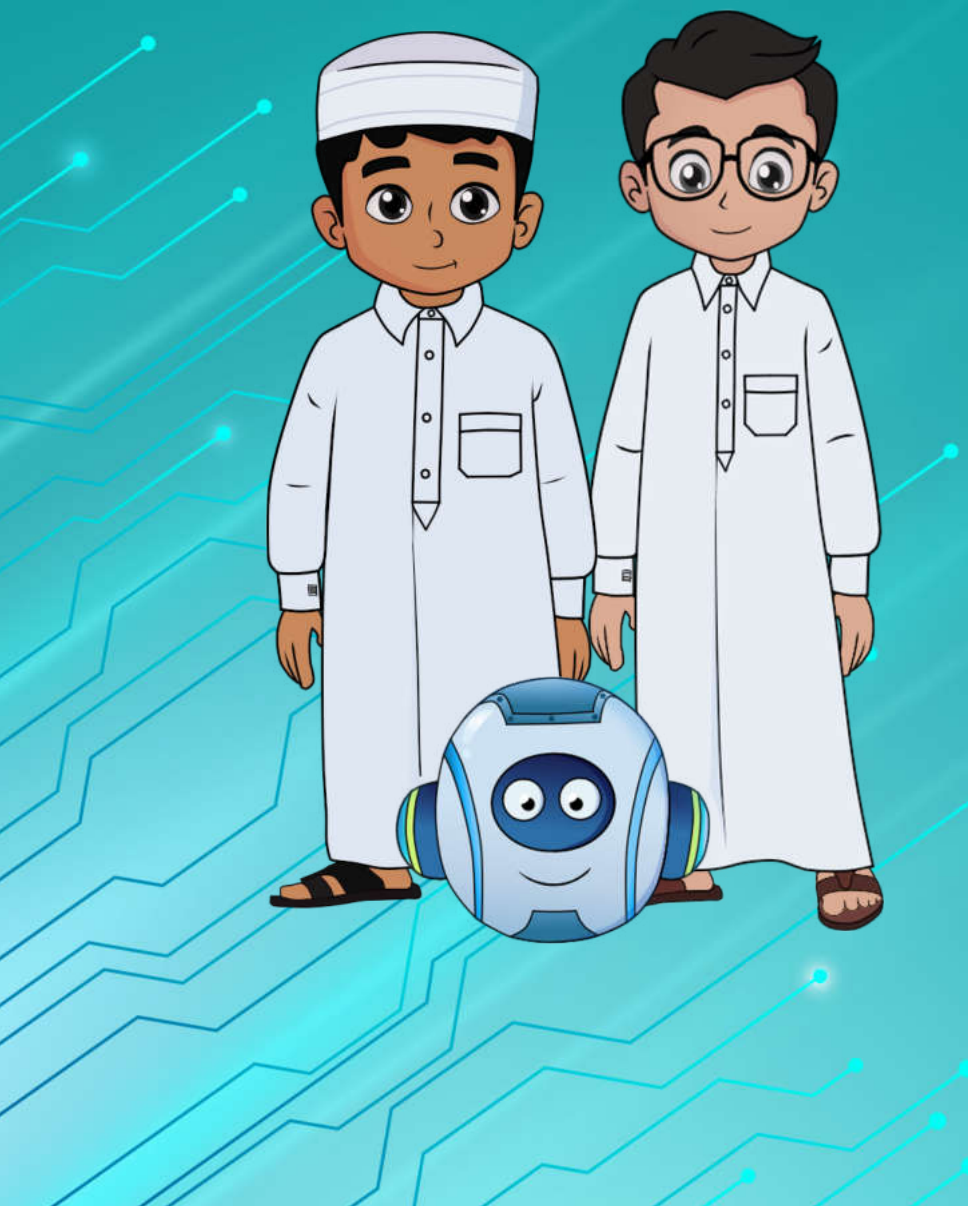
يَلْجَأ القَراصِنَة والمُحتالون إلى خرق الحاسوب بالبرمجيَّات والرَّوابِط الخبيثة؛ ما يؤدِّي إلى تَوَقُّفه عن العمل، ثمّ يَبْتَزُّون الضَّحايا من أجل دَفْع المال مقابل استرجاع إمكانيَّة الدُّخول إليه.

التِّجارة الإلكترونيَّة

يمكن أن يزور المُستخدِم موقعًا مزيَّفًا بهَدَف شراء بعض السِّلَع؛ إلَّا أنَّه يُفَاجَأ بوقوعه ضحيَّة للاحتيال والنَّصب عبر الإنترنت، وهو ما يعني أنَّه سيدفع المال دون الحصول على أيّ مقابل.

استغلال الكوارث

في أوقات الأزمات، مثل الكوارث الطَّبيعيَّة أو الصِّحِّيَّة مثل "جائحة كورونا"، يَلْجَأ مُرْتَكِبو الجرائم الإلكترونيَّة إلى تنظيم حملات وهميَّة تدعو إلى التَّبرُّع من أجل مساعدة الضَّحايا، ما يتسبَّب في إعطائهم معلومات خاصَّة بالحسابات البنكيَّة، وهو ما يَقَع تحت طائلة الاحتيال عبر الإنترنت.



الفَصْل الثَّاني

كيفيَّة تنفيذ عمليَّات الاحتيال عبر الإنترنت

أوَّلًا

الثَّغَرات المُساعِدَة على عمليَّات الاحتيال عبر الإنترنت

تعريف الثَّغْرة الأمنيَّة

مصطلح يُطلَق على مناطق ضعيفة في أنظمة تشغيل الحاسوب والبرمجيَّات، وهذه المناطق الضَّعيفة يمكن التَّسَلُّل عبرها إلى داخل نظام التَّشغيل، ومِن ثَمَّ يتمّ التَّعديل فيه لتدميره نهائيًّا، أو للتَّجسُّس على المعلومات الخاصَّة بصاحب الحاسوب المُختَرَق، أو ما يُعرَف بجهاز الضَّحيَّة.

ثَغْرة Zero-Day

واحدة من عيوب النُّظُم الإلكترونيَّة، وهي ثغرة في البرامج يمكن استغلالها مِن قِبَل المُتَسَلِّلين الذين ليس لديهم تصريح حتى الآن؛ حيث لا يعرف مُطَوِّرو البرامج مكان الضَّعف أو يُطوِّرون إصلاحًا له، أو أنَّهم يتجاهلون ذلك، وتؤدِّي هذه الثَّغرة الأمنيَّة إلى خَرْقٍ شديد الخطورة للأمن السِّيبرانيّ.

آليّة عمل هجوم الثَّغرات غير المُكتَشَفة Zero-Day

1
البحث عن الثَّغرات الأمنيَّة.

2
إنشاء رمز الاستغلال.

3
البحث عن الأنظمة المُتأثِّرة بالثَّغرة الأمنيَّة.

4
التَّخطيط للهجوم.

5
التَّسَلُّل.

6
إطلاق الثَّغرات غير المُكتَشَفة Zero-Day.

الهجمات غير المُستهدِفَة لثَغرة Zero-Day

عادةً ما يتمّ شَنّ هجمات Zero-Day غير المُستهدِفة ضِدّ عدد كبير من مُستخدِمي المنزل (الأفراد العاديِّين) الذين يستخدمون نظامًا ضعيفًا، مثل نظام التَّشغيل أو المُتصفِّح، وغالبًا ما يكون هدف المُهاجِم هو اختراق هذه الأنظمة واستخدامها لبناء شبكات روبوت ضخمة لتنفيذ جرائم إلكترونيَّة أكبر فيما بعد.

ثانيًا
أمن البيانات الشَّخصيَّة والاحتيال عبر الإنترنت

أمان المعلومات

هو مجموعة من الإجراءات والأدوات الأمنيَّة التي تَحْمِي على نطاق واسع المعلومات الحسَّاسة من سُوء الاستخدام أو الوصول غير المُصَرَّح به أو التَّعطيل أو الإتلاف.

سرقة البيانات

هي عمليَّة سرقة معلومات رقميَّة مُخَزَّنة على أجهزة الحاسوب أو الهواتف؛ للحصول على معلومات سِرِّيَّة أو انتهاك الخصوصيَّة، مثل: معلومات الحساب المَصْرفيّ، وكلمات المرور على الإنترنت، ورقم جواز السَّفر، والسِّجلَّات الطِّبيَّة والاشتراكات عبر الإنترنت، وما إلى ذلك.

ويُطلَق على كلمة "سرقة" في عالَم الإنترنت مصطلح "انتهاك البيانات" أو "تَسَرُّب البيانات".

ثالثًا: البَصْمَة الرَّقميَّة والاحتيال عبر الإنترنت

يُشير مصطلح "البَصْمَة الرَّقميَّة" أو الظِّلّ الرَّقميّ أو البَصْمَة الإلكترونيَّة، إلى أثر البيانات التي تتركها عند استخدام الإنترنت، وهي تشمل مواقع الويب التي تَزُورُها، ورسائل البريد الإلكترونيّ التي تُرْسِلها وتَسْتَقْبِلها، والمعلومات التي تُقَدِّمها عبر الإنترنت.

على سبيل المثال: ما يقوم به الشَّخص من النَّشر على وسائل التَّواصُل الاجتماعيّ أو الاشتراك في الرَّسائل الإخباريَّة أو تَرْك مُراجعة على الإنترنت أو التَّسوُّق عبر الإنترنت، كلُّها أنشطة تُشَكِّل "البَصْمَة الرَّقميَّة".

وهناك نوعان من
البَصْمـات الرَّقميَّـة
أحدهما نَشِـط والآخر
غير نَشِـط

البَصْمَات الرَّقميَّة النَّشِطة

يُقْصَد بها مشارَكة المُستخدِم معلومات عن نفسه عمدًا، من خلال النَّشْر أو المشارَكة على مواقع شبكات التَّواصُل الاجتماعيّ أو المنتديات عبر الإنترنت.

البَصْمَات الرَّقميَّة غير النَّشِطة

يتمّ إنشاء البَصْمَة الرَّقميَّة غير النَّشِطة عندما يتمّ جَمْع معلومات حول المُستخدِم دون أن يُدرِك أنَّ هذا يَحْدُث.

الآثار السَّلبيَّة للبَصْمَة الرَّقميَّة

1

تُعَدّ بيانات دائمةً نسبيًّا؛ وتُصبِح متاحةً للاطلاع العامّ أو الجزئيّ.

2

يمكن للبَصْمَة الرَّقميَّة أن تُحدِّد سُمْعة الشَّخص، كما هو الحال على أرض الواقع.

3

يمكن إساءة تفسير الكلمات والصُّور التي يَنْشُرها الفرد عبر الإنترنت أو تغييرها، ما يتسبَّب في إهانة غير مقصودة.

4

يمكن للمحتوى المُخصَّص لمجموعة خاصَّة أن ينتشر خارجها، ما قد يَضُرّ بالعلاقات بين الأفراد.

5

يستطيع مُجْرمو الإنترنت استغلال بصمتك الرَّقميَّة لأغراض مثل الانتحال عبر الإنترنت، للوصول إلى الحساب أو إنشاء هُويَّات مُزيَّفة بناءً على بياناتك الشَّخصيَّة وخِداع الآخرين.

أمثلة على البَصْمَة الرَّقميَّة

من بين الطُّرق التي يُضيف بها المُستخدِمون إلى بصمتهم الرَّقميَّة ما يلي:

- التَّسوُّق عبر الإنترنت.
- التَّسجيل لإنشاء حساب على موقع ويب معيَّن.
- تنزيل التَّطبيقات واستخدامها.
- التَّسجيل من أجل النَّشرات الإخباريَّة للعلامات التِّجاريَّة.
- الخدمات البنكيَّة عبر الإنترنت.
- الاشتراك في المطبوعات والمُدوَّنات.
- استخدام وسائل التَّواصُل الاجتماعيّ على الأجهزة الخاصَّة بك.
- تسجيل الدُّخول إلى مواقع الويب الأخرى باستخدام بيانات اعتماد وسائل التَّواصُل الاجتماعيّ.
- التَّواصُل مع الأصدقاء وجِهات الاتِّصال عبر الإنترنت.
- مشارَكة المعلومات والبيانات والصُّور مع معارفك.
- الاشتراك في مصدر إخباريّ عبر الإنترنت.

حماية البَصْمَة الرَّقميَّة

- استخدام مُحرِّكات البحث للتَّحقُّق من البَصْمَة الرَّقميَّة.
- تقليل عدد مصادر المعلومات، فعلى سبيل المثال، قد تحتوي مواقع الويب على معلومات أكثر ممَّا قد يرغب الفرد في عَرْضِه، مثل رقم الهاتف والعنوان والعمر، لذا على المُستخدِم إزالة المعلومات الشَّخصيَّة منها.
- تقييد كمِّيَّة البيانات التي يتمّ مشاركتها.
- التَّحقُّق من إعدادات الخصوصيَّة.
- تجنُّب الإفراط في المُشارَكة عبر وسائل التَّواصُل الاجتماعيّ.
- تجنُّب المواقع غير الآمِنَة.
- عدم الكَشْف عن البيانات الخاصَّة على شبكة Wi-Fi عامَّة.
- حَذْف الحسابات القديمة.

- إنشاء كلمات مرور قويَّة وتغييرها من حين إلى آخر واستخدام Password Manager.
- عدم تسجيل الدُّخول إلى مواقع الويب والتَّطبيقات باستخدام Facebook.
- تحديث البرامج دوريًّا.
- مراجعة استخدام الهاتف المحمول بتعيين رمز مرور للجهاز.
- التَّفكير جيِّدًا قبل النَّشْر.
- التَّحَرُّك بسرعة بعد انتهاك البيانات.

الفَصْل الثَّالث

كيفيَّة التَّصرُّف في حال التَّعرُّض للاحتيال عَبْر الإنترنت

أوَّلًا: إرشادات الحماية من الاحتيال عبر الإنترنت

1. تَحْميل التَّطبيقات من المتاجِر المعروفة.
2. تَحْديث الهاتف باستمرار.
3. تَجنُّب الرَّوابِط مجهولة المَصْدر.
4. الحَذَر من المُعاملات التي تَتَضمَّن أطرافًا مجهولة.
5. الاستعانة ببرامج مُكافَحَة الفيروسات.
6. استخدام كلمات مرور قويَّة وتغييرها من حين إلى آخر.
7. عدم التَّسوُّق من المواقع المجهولة.

ثانيًا: حماية البيانات من الاحتيال عبر الإنترنت

- كن مُتيقِّظًا لعمليَّات الاحتيال عندما تتعامل مع اتِّصالات مُتطفِّلة.
- إذا تعرَّفت إلى شخص ما عبر الإنترنت، فخُذْ وقتًا لتقوم ببعض الأبحاث الإضافيَّة عنه.
- لا تفتح نصوصًا أو نوافذ تظهر أمامك أو رسائل إلكترونيَّة غير موثوقة.
- احتفظ بتفاصيلك الشَّخصيَّة بشَكْلٍ آمنٍ، مثل وَضْع قُفْل على صندوق بريدك.
- حَافِظ على هاتفك والحاسوب الخاصّ بك بشَكْلٍ آمنٍ عَبْر إنشاء كلمة سِرٍّ قويَّةٍ، وتحديث أنظمة التَّشغيل باستمرار، والاحتفاظ بنُسخةٍ احتياطيَّةٍ للمحتوى.
- احْمِ شبكتك الخاصَّة بالـWi-Fi بوَضْع كلمة سِرّ عليها.
- راجِع ترتيباتك المُتَعلِّقة بالخصوصيَّة والأمان على مواقع التَّواصُل الاجتماعيّ.
- احْذَر أيّ طلباتٍ تَتَعلَّق بتفاصيلك أو مالك.

- كن حَذِرًا عندما تَتَسَوَّق على الإنترنت، وخاصَّة مع العروض التي تبدو مُغريةً جدًّا.
- غَيِّر كلمات السِّرّ الخاصَّة بك على الإنترنت إذا كنت تعتقد أنّ الحاسوب الخاصّ بك أو الهاتف قد تَعَرَّض للقَرْصَنَة.
- ضَعْ إشارةً مرجعيَّةً للمواقع المهمَّة التي تقوم بزيارتها باستمرار.
- تَذَكَّر أنّ رسائل الخطأ الحقيقيَّة من مايكروسوفت Microsoft أو الشَّركات التِّقنيَّة الكبيرة الأخرى، لا تَتَضَمَّن أبدًا أرقام هواتف لكي تتَّصل بها.
- تَذَكَّر: لن تتَّصل بك مايكروسوفت Microsoft وشركات التِّقنيَّة الشَّرعيَّة الأخرى أبدًا لتُخبِرك أنّ هناك مشكلة في جهازك.
- إذا كانت شاشتك تمتلئ بشَكْلٍ مفاجئٍ بالنَّوافذ المنبثقة المخيفة، فيجب إغلاق الحاسوب فورًا.

ثالثًا: كيفيَّة التَّصرُّف عند التَّعرُّض للاحتيال عَبْر الإنترنت

- **أوَّلًا:** عليك عدم التَّواصُل مع الشَّخص المُحتال.
- **ثانيًا:** عليك غَلْق جميع الحِسابات المفتوحة في وقت تلقِّي الرِّسالة التَّحذيريَّة أو عند الشَّكّ في تَعَرُّض أيّ من حِساباتك للاختراق، أو عند تلقِّي رسالة تهديد وابتزاز من مجهول، وكذلك إغلاق الأجهزة.
- **ثالثًا:** الاحتفاظ بنَصّ الرِّسالة المُرسَلة؛ لكونه دليلًا يُدِين المُتَسَلِّل.
- **رابعًا:** يجب إبلاغ شخصٍ تَثِق به، مثل الوَالِدَين أو أحد المُشْرِفين في المدرسة.
- **خامسًا:** عدم مجاراة المُتَسَلِّل؛ لأنَّه شخص مُحترِف في ترهيب الآخرين، ولا تَرْضَخْ لطلباته أيضًا مثل إرسال المال، كما يَحْدُث في هجمات الفدية.
- **سادسًا:** عدم تَصْدِيق ما يقوله المُتَسَلِّل، وعدم ترك مجال له للتَّلاعُب بأعصابك.
- **سابعًا:** أيّ معلومات تعرفها أو رقم يَخُصّ هذا المُتَسَلِّل أو أيّ رسائل أُرْسِلت إليك؛ عليك تَقْدِيمها إلى أشخاص محلّ ثقة؛ ليتمكَّنوا من تقديمها إلى إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية.

أمثلة على أشهر عمليَّات الاحتيال عبر الإنترنت

المثال الأوَّل
شركة تويوتا بوشوكو

CyberEco

TOYOTA BOSHOKU

في عام 2019م تَعَرَّضَتْ شركة "تويوتا بوشوكو" التي تعمل على توريد سيَّارات تويوتا وتزويدها ببعض المُعدَّات لعمليَّة احتيال عَبْر الإنترنت بَلَغَتْ قِيمَتها حوالي 37 مليون دولار أمريكيّ؛ إذ أَقْنَع المُحتالون الإلكترونيُّون المدير الماليّ للشَّركة بتغيير معلومات الحساب المَصرفيّ للمُستَلِم، وهو ما سَاعَدهم على الحصول على هذه الأموال.

المثال الثَّاني

العُملات الرَّقميَّة

في عام 2017م، فَقَدَ كثير من الأشخاص آلاف الدُّولارات بعد أن فَقَدُوا عُملات رقميَّة من نوع "إيثريوم"؛ فقد اخْتَرَقَ المُهاجِمون محفظة العُملة، وقاموا بتحويلها نحو خوادمهم الخاصَّة.

وفي العام نفسه (2017م)، انْتَشَرَ فيروس أُطْلِق عليه "WannaCry" أو "هجوم طَلَبِ الفِديَة"، الذي تسبَّب في تعطيل الحواسيب، ومن أجل استعادة إمكانيَّة الدُّخول؛ طَالَب المُخْتَرِقون أصحاب الأجهزة بدَفْع مبلغٍ من المال على شكل عُملة (بيتكوين) لصعوبة اقتفاء أَثَرها، وبالتَّالي الهَرَب بفَعْلَتهم دون عقابٍ.

CyberEco

المثال الثَّالث
شركة ياهو

خلال الفترة المُمتدَّة بين عامَي 2013م و2016م، تَعَرَّضَتْ شركة ياهو إلى سرقة بيانات حوالي 3 مليارات مستخدِمٍ؛ حيث تَمَكَّن المُهاجِمون من الوصول إلى معلومات وكلمات مرور يمكن استخدامها في الوصول إلى خدمات وحِسابات أخرى على الإنترنت.

المثال الرَّابع

سرقة الأموال في روسيا

انْتَشَرَ في روسيا بين عامَي 2013م و2014م واحد من أبرز أساليب الاحتيال عبر الإنترنت؛ حيث يقوم أحد المُحتالين بالاتِّصال بضحيَّته، وسرقة هوية موظَّف في البنك الذي يتعامل معه المُستهدَف، ويَطْلُب منه معلومات تَتَعَلَّق بالبطاقة المَصرفيَّة، بحجَّة إيقاف معاملات ماليَّة غير طبيعية، وبعد حصول المُحتال على بيانات البطاقة يقوم باستغلالها لسرقة الأموال وتحويلها إلى حِسابات تَخُصُّه.

المثال الخامس

سرقة 600 مليون دولار في عمليَّة احتيال ضخمة بالعُملات الرَّقميَّة

قام قَراصِنَة إلكترونيُّون بسرقة حوالي 600 مليون دولار، في واحدة من كبرى عمليَّات الاحتيال في تاريخ العُملات الرَّقميَّة؛ وقد اسْتَغَلّ القَراصِنَة ثغرةً أمنيَّةً في نظام تلك العُملة لسرقة الأموال التي تعود لعشرات الآلاف من أعضاء مجتمع التَّشْفير.

التمارين والتدريبات

انْتَبِه!

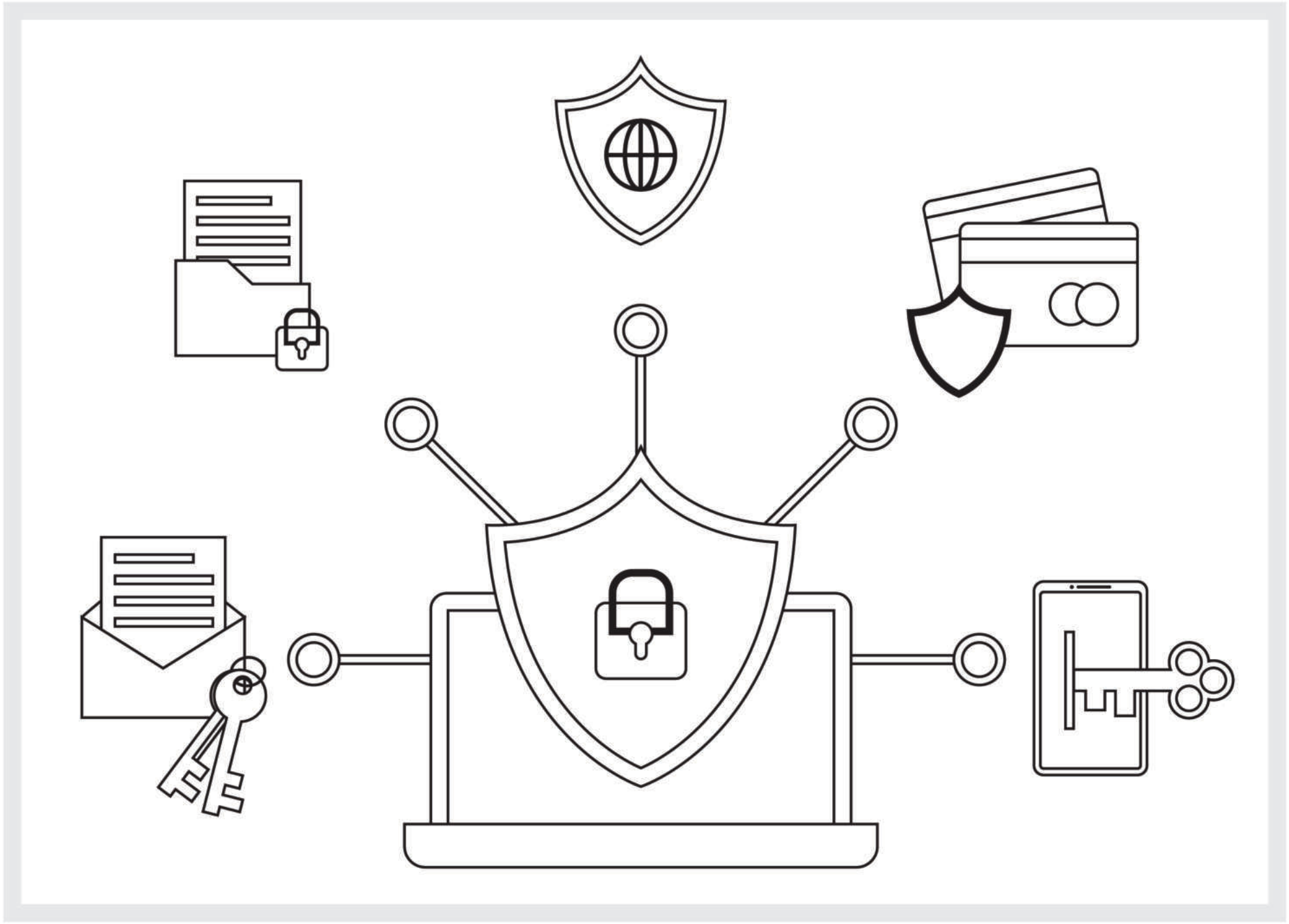
الاحتيال عبر الإنترنت

نوع من أنواع الخِداع والحيل التي تتمّ على شبكة الإنترنت، وغالبًا ما تَحدُث هذه الجرائم في غرف الدَّردشة أو عبر البريد الإلكترونيّ أو على المنتديات أو مواقع الإنترنت (الويب)، والهدف من هذه الجرائم هو الاحتيال على العملاء والمُستخدِمين عن طريق سرقة الأموال والمعلومات الشَّخصيَّة المهمَّة وغيرها من الأغراض الأخرى.

أولًا: التَّمَارين الصَّفِّيَّة

هل تعلم؟

غالبيَّة الجوائز والهدايا التي تأتي عن طريق الإنترنت دون سببٍ تكون بدايةً لعمليَّة احتيال عبر الإنترنت.



التَّمرين الأوَّل

ضع علامة (✓) بجانب العبارة الصَّحيحة، أو علامة (✗) بجانب العبارة الخاطئة:

توجيه

اقْرأ الجمل الواردة بتمعُّن، ثمّ حدِّد ما إذا كانت الجملة صحيحة أم خاطئة، ويوجد مثال محلول.

1. جريمة الاحتيال عبر الإنترنت هي تلاعب متعمَّد في المعلومات والبيانات الموجودة على الحاسوب والأجهزة الذكية. ✓

2. جريمة الاحتيال عبر الإنترنت هي الدُّخول المُصرَّح به من أجل الحصول على معلومات وبيانات موجودة على الحاسب الآليّ. ☐

3. يُعَدّ الدُّخول على الأجهزة أو الأنظمة من أجل الحصول على ربح غير مشروع أو إلحاق ضررٍ ما بها من أنواع جرائم الاحتيال عبر الإنترنت. ☐

4. تُساعِد التِّقنيَّة الحديثة مُرْتكبي جرائم الاحتيال عبر الإنترنت على ارتكاب الجرائم على النِّطاق المحلِّيّ فقط. ☐

5 الاحتيال عبر الإنترنت هو استعمال الأنظمة والأجهزة المُصرَّح بها للنَّصْب والاحتيال على الآخرين.

6 الاحتيال المعلوماتيّ هو الغِشّ والخِداع المعلوماتيّ من خلال التَّلاعب بأنظمة المُعالَجة الآليَّة للمعلومات دون وجه حقّ، من أجل الحصول على الخدمات أو الأموال أو الأصول.

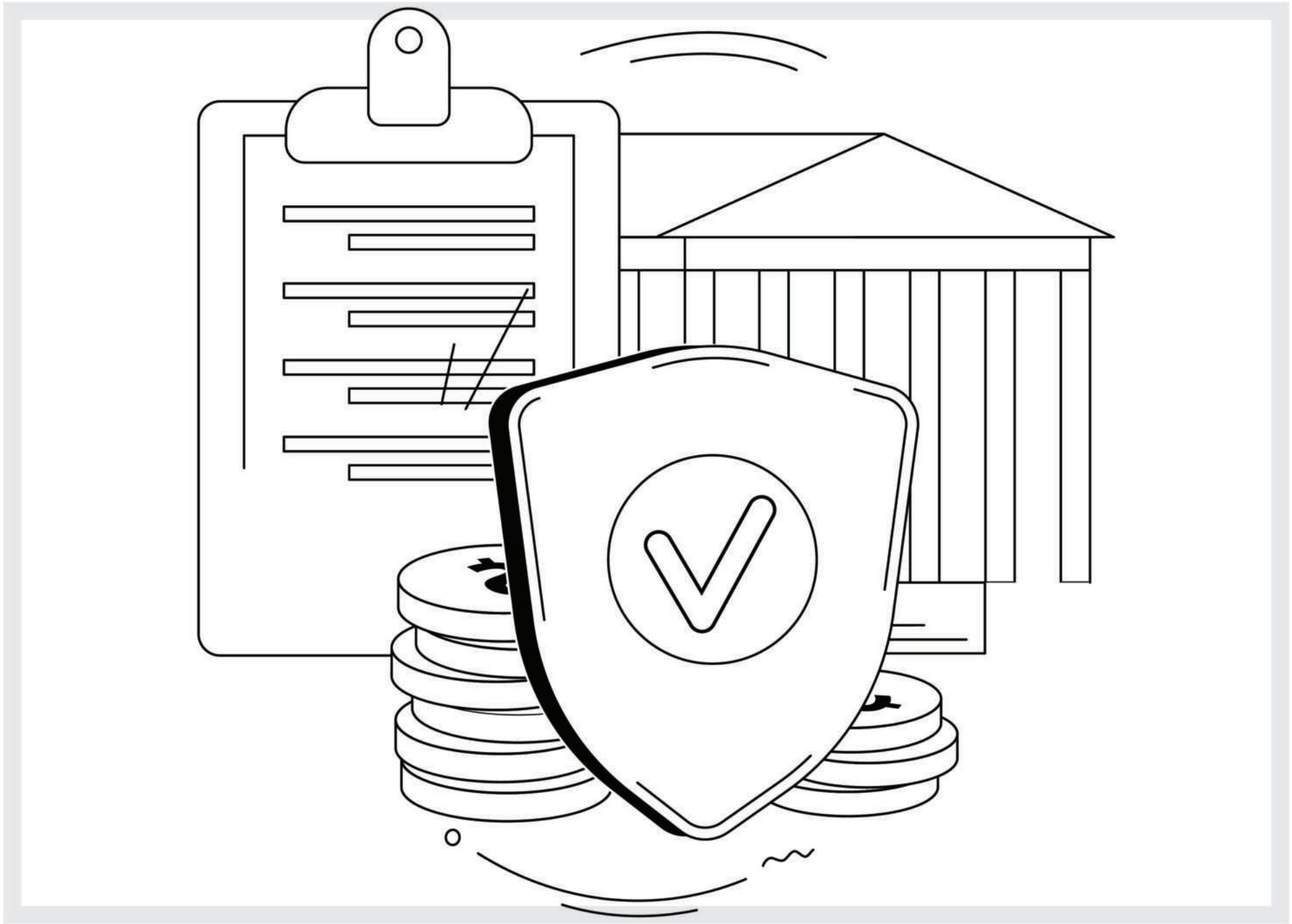
7 النَّصْب عبر الإنترنت هو الحصول على الأموال بطُرق غير مشروعة من خارج الدَّولة فقط.

8 يَستخدِم الجُناة في الاحتيال عبر الإنترنت التِّقنيّات بطريقة مشروعة ودون أيّ تلاعب.

انْتَبِه!

النَّصْب عبر الإنترنت

الاستيلاء على مال الآخرين بوسيلةٍ يَشُوبها الخِداع، ما يتسبَّب في تَسَلُّم هذا المال عن طريق أجهزة الحاسوب والأجهزة الذَّكيَّة.



هل تعلم؟

تُحَدِّد البصمة الرَّقميَّة سُمْعة الأشخاص على الإنترنت كما يَحْدُث في الحياة العاديَّة.

التَّمْرين الثَّاني

صِل المُصْطَلَحَات والعبارات من العمود (أ) بما يُناسبها من العمود (ب):

توجيه

اقرأ الجمل الواردة في الجدول بتَمَعُّن، وابدأ بالجملة الأُولَى في العمود (أ)، وابحث في العمود (ب) عن الجملة التي تستكمل معناها، وأدناه مثال عن الوصل بين جملتين.

العمود (أ)	العمود (ب)
الاحتيال عبر الرَّسائل النَّصِّيَّة القصيرة	نوع من أنواع الاحتيال عبر الإنترنت، حينما يتمّ تهديد الضَّحيَّة بإتلاف البيانات أو دَفْع فدية.
الاحتيال عبر الإعلانات	يعتمد على خِداع الآخرين عبر برامج تغيير الصَّوت لإقناع الضَّحايا بمشاركة البيانات والمعلومات الشَّخصيَّة.
فيروسات الفدية	يتمّ في أثناء تسوُّق الضَّحيَّة، وبعد دفع قيمة المُنتَج لا يَصِل إليه أيّ شيء، أو ربَّما يَصِل إليه مُنتَج خاطئ أو مُقَلَّد.
الاحتيال بسرقة بطاقات الائتمان	تُستغلّ فيه أسماء جمعيَّات خيريَّة وهميَّة من أجل الحصول على الأموال عن طريق إثارة تعاطف الآخرين.
الاحتيال الصَّوتي	يتمّ إرسال رابطٍ من خلال رسالة نصِّيَّة، وبمجرَّد الضَّغط عليه تتمّ عمليَّة الاحتيال.
احتيال التَّسوُّق عبر الإنترنت	يتمّ فيه إيهام البائع بأنّ المشتري قام بالدَّفع وبعد إرسال المُنتَج لا تُضاف الأموال إلى رصيده.
الاحتيال بجمع التَّبرُّعات	يتمّ من خلال سَرِقَة بيانات بطاقات الائتمان واستخدامها في شراء المُنتجَات عبر الإنترنت.
الاحتيال على البائع عبر الإنترنت	الإعلانات الخبيثة المُحمَّلة بالفيروسات، التي تُستخدَم في سرقة المعلومات والبيانات.

التَّمرين الثَّالث

امْلأ الفراغات بالكلمات المناسِبَة:

توجيه

اقْرأ الجمل الواردة أدناه بتمعُّن، وحدِّد الكلمات المناسبة لملء الفراغ؛ بحيث يُصبح للجملة معنًى مفيدٌ، وأدناه مثال محلول.

1. يُعَدّ الاحتيال لسرقة الهُويَّة أخطر أنواع الاحتيال عبر الإنترنت؛ حيث يقوم المُجْرم بسرقة ..... **البيانات** ..... الشَّخصيَّة، مثل الاسم وتاريخ ..... **الميلاد** ..... وعنوان ..... **الإقامة** ..... وتفاصيل الحساب ..... **البنكيّ** ..... وكافَّة المعلومات المهمَّة الأخرى.

2. تُستخدَم تلك المعلومات في سرقة ..... ويمكن أن يتمّ استغلال الهُويَّة في فتح ..... بنكيَّة، أو الحصول على بطاقات ..... أو قروض، أو من أجل تسجيل خطوط .....

3. يمكن لمُجْرمي الاحتيال عبر الإنترنت سرقة ..... الشَّخصيَّة للاستيلاء على ..... البنكيَّة المفتوحة بالفعل للشَّخص، عن طريق ..... شخصيَّته.

4. لا بُدّ أن تتجنَّب إعطاء الآخرين أيّ ..... شخصيَّة، كما يجب أن تحذف أيّ مستندٍ أو ملفٍّ يحتوي على ..... سرِّيَّة أو أرقام بطاقات ..... قبل التَّخلُّص منه.

5 اطلب من البنك الذي تتعامل معه أن يُرسل إليك إشعارًا أو ..... معك في حال كان هناك شكّ في أيّ معاملة غريبة أو غير معتادة على .....البنكيّ.

6 عليك أن تنتبه جيدًا في تعاملاتك مع ..... التّجاريّة، أو مع الآخرين، سواءٌ من خلال الهاتف أو .....أو الإنترنت بشَكلٍ عامٍّ، خاصَّةً مِنصّات .....

7 تجنَّب فتح أيّ ..... غير موثوقة، وقُم بإلغاء ..... المنبثقة، وتأكَّد من ..... الشَّخص الذي تتحدَّث إليه عبر الإنترنت.

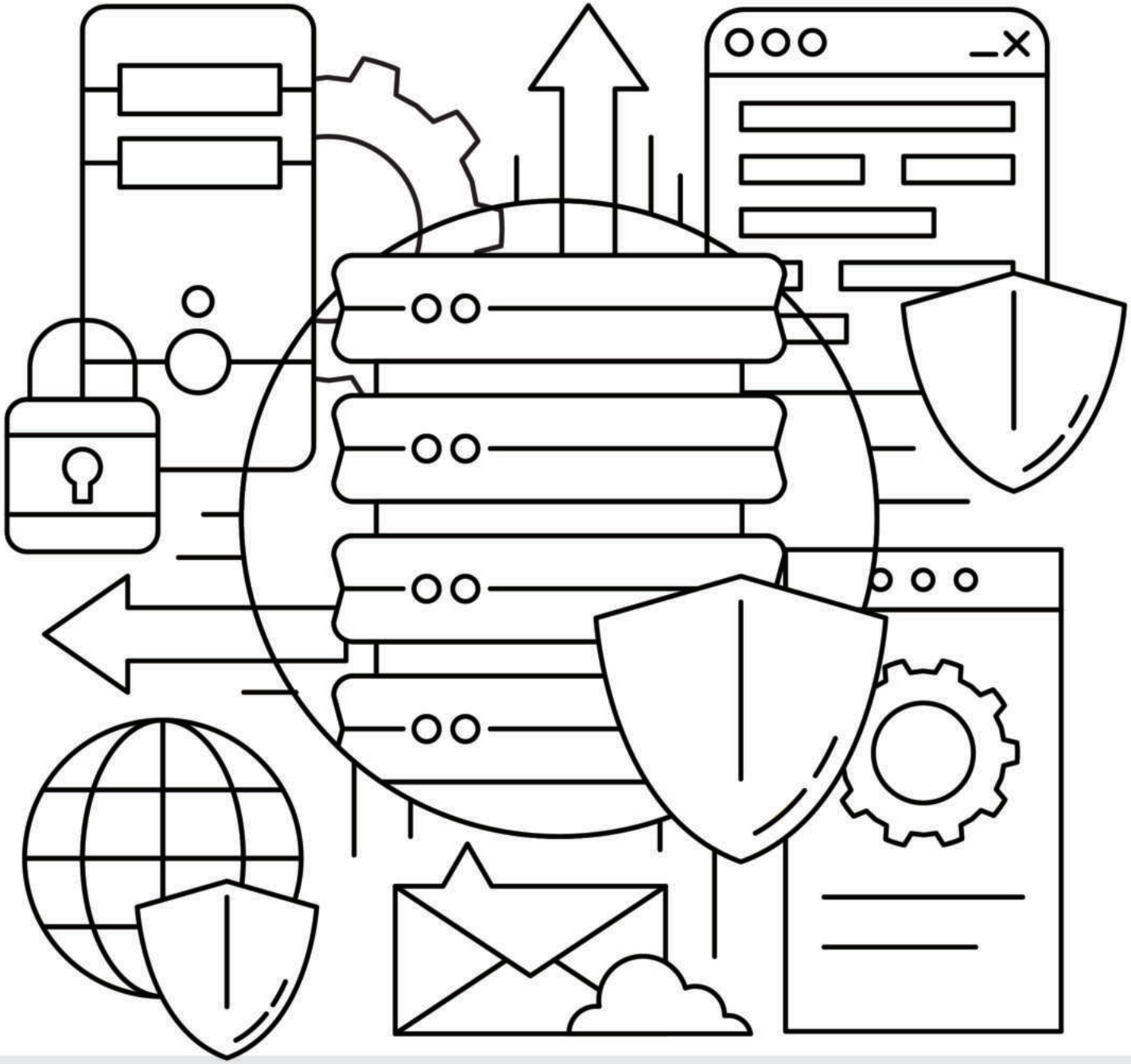
8 استخدم ..... قويَّة على هاتفك وحساباتك الشَّخصيَّة، ولا تُشارِكها مع الآخرين، ولا تنسَ الاحتفاظ ..... احتياطيَّة لبياناتك، وتجنَّب استخدام شبكات ..... العامَّة، خاصَّةً إذا كنت ستفتح أيّ تطبيق له علاقة بمعاملاتك البنكيَّة.

9 إذا كنت ترغب في التَّسوُّق ..... فعليك أن تتأكَّد من الثِّقة بهذا المتجر، وأن تقرأ تقييمات الآخرين ومراجعاتهم، ومن الأفضل التَّعامل مع المتاجر المشهورة والتي تُعرَف بالأمان.

انْتَبِه!

الاحتيال المعلوماتيّ

الخِداع أو الغِشّ المعلوماتيّ الذي يقوم على التّلاعب في نُظُم المُعالَجة الآليَّة للمعلومات، بغرض الحصول دون وجه حقّ على خدمات أو أموال أو أصول معيَّنة.



التَّمرين الرَّابع

ضع علامة (✓) أو علامة (✗) أمام العبارات التالية:

توجيه

اقْرأ الجمل الواردة في الجدول بتمعُّن، وحَدِّد ما إذا كانت الجمل تُعَبِّر عن معلومات صحيحة أم خاطئة في مجال الحماية من الاحتيال عبر الإنترنت، وفي حال كانت صحيحة ضع بجانبها علامة (✓) ، وإذا كانت خاطئة ضع علامة (✗) ، وأدناه مثال محلول.

1	لا بُدّ من استخدام النُّسخ القانونيَّة من التَّطبيقات البنكيَّة.	✓
2	يمكنك تحميل التَّطبيقات من أيّ موقع من مواقع الإنترنت.	
3	يجب ألَّا تذكر بياناتك السِّرِّيَّة والمعلومات الخاصَّة بك في أثناء الاتِّصالات الهاتفيَّة.	
4	يمكنك أن تضغط على أيّ روابط يُرسِلها إليك الأصدقاء، سواءً في الرَّسائل النَّصِّيَّة أم عبر البريد الإلكترونيّ.	
5	الاستعانة بأطراف مجهولة في المعاملات الماليَّة قد تُعرِّضك لعمليَّة نصب أو تبييض أموال.	

6	استخدام برامج مكافحة الفيروسات عامل أساسيّ في حمايتك من الاحتيال عبر الإنترنت.
7	يمكنك تكرار اسمك أو كتابة تاريخ ميلادك ككلمة مرور قويّة لحساباتك وأجهزتك.
8	يجب تحرّي الدّقّة في أثناء التّسوّق عبر الإنترنت، ويُفضّل التّعامل مع المواقع المعروفة.
9	يمكنك كتابة بيانات بطاقاتك البنكيّة على أيّ تطبيق عبر الإنترنت.
10	تجنّب استخدام النُّسخ المُعدّلة أو المُخترقة من التّطبيقات الخاصّة بالهواتف الذّكيّة.

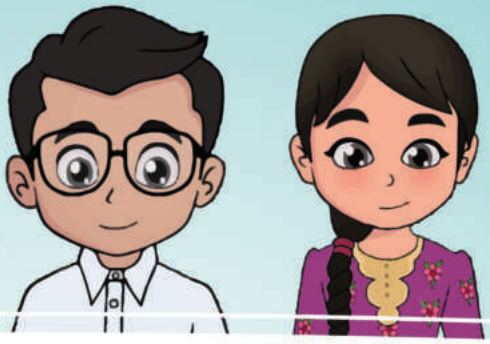
انْتَبِه!

أسباب الوقوع ضحيَّةً للاحتيال عبر الإنترنت

- قلَّة وَعْي الأفراد حول كيفيَّة استخدام وسائل التَّواصل الاجتماعيّ ومواقع الإنترنت.
- الدُّخول إلى مواقع إلكترونيَّة غير آمنة.
- نَشْر الأفراد معلومات شخصيَّة عن أنفسهم عبر مواقع التَّواصل والإنترنت.
- التَّعامُل مع المتاجِر الإلكترونيَّة غير الموثوقة.
- انتحال المُتسلِّلين صفة شخصيَّات معروفة وذات مكانةٍ، مثل شخصيَّات موظَّفي الحكومة أو الخبراء أو المسؤولين التَّنفيذيِّين أو التِّقنيِّين.
- استغلال مشاعر التَّعاطف، مثل حالات الطَّوارئ؛ لجذب تعاطف الضَّحيَّة المُستهدَفة عبر الإنترنت.

التَّمرين الـخامــس

ضَع الكلمة المناسبة
أمام كلّ جملة:



توجيه

اقْرأ الجمل الـواردة في الجـدول بتمعُّـن، وفكِّـر في كـلمـة أو عـبـارة تُعَبِّر عـن مـعنى الجـمـلـة، واكْتُبها في العمود الثَّاني، وأدناه مثال محلول.

1. الأثر الذي تتركه خَلفك والمعلومات التي تُخَلِّفها بعد كلّ استخدام للإنترنت.	**البَصْمة الرَّقميَّة**
2. النَّصْب وسرقة البيانات باستخدام تقنيَّات التِّكنولوجيا والإنترنت.	
3. برامج تُساعِدك على حماية أجهزتك وصَدّ هجمات المُحتالين.	
4. مجموعة من الحروف والرُّموز والأرقام التي تُستخدَم لحماية حساباتك.	
5. الاستعانة بوسيطٍ من أجل تحويل الأموال من طرفٍ إلى طرفٍ.	

انْتَبِه!

الثَّغرة الأمنيَّة

مصطلح يُطلَق على نقاط ضعف في أنظمة تشغيل الحواسيب والهواتف الذكيَّة والأجهزة اللّوحيَّة، والتي يَتَسلَّل عبرها المُهاجِمون إلى داخل نظام التَّشغيل، ومن ثمّ يتمّ التَّعديل فيه لتدميره نهائيًّا، أو للتَّجسُّس على المعلومات الخاصَّة بصاحب الحاسوب المُختَرَق، أو ما يُعرَف بجهاز الضَّحيَّة.


ثانيًا: التَّمارين اللَّاصَفِّيَّة

انْتَبِه!

ثغرة Zero-Day

هي ثغرة في برامج الحاسوب يمكن استغلالها من قِبل المُتسلِّلين، وتؤدِّي هذه الثَّغرة الأمنيَّة إلى خرقٍ شديد الخطورة على الأمن السِّيبرانيّ.

التَّمْرين الأوَّل

استخـرج الـكلمـات التَّالية من الـجـدول:

توجيه

اقْرأ الكلمات الواردة أدناه بتمعُّن، وابحث في الجدول عن حروف متتالية تُشكِّل هذه الكلمات، وأدناه مثال عن كلمة **"النَّصْب"** وكيف تمّ إيجاد أحرف الكلمة في الجدول:

ض	ا	ي	س	ا	ل	ن	ص	ب	ك
ا	ل	أ	و	ا	م	ر	غ	ي	ف
ش	ت	ك	ك	ل	إ	ف	ل	ا	س
ا	ل	ا	ح	ت	ي	ا	ل	ن	ش
ه	ا	ش	ق	ق	ب	خ	د	ا	ع
و	ع	ل	م	ن	م	ش	م	ت	غ
و	ب	ج	ر	ي	م	ة	ق	ض	ش
م	ج	ر	م	ة	ا	ل	ض	ر	ر

الاحتيال - النَّصْب - التَّلاعب - بيانات - الأوامر - التِّقنيَّة - الضَّرر

جريمة - مُجْرم - خِداع - غِشّ - إفلاس - حَقّ

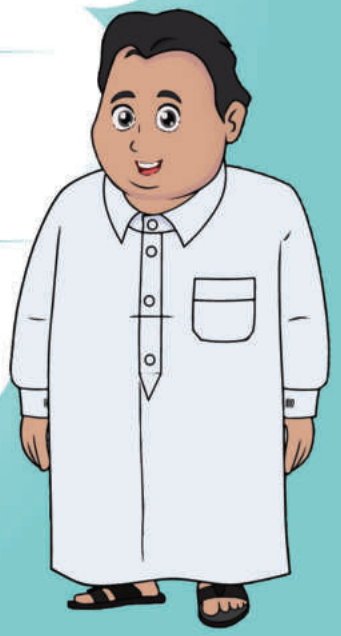
التَّمرين الثَّاني

حدد الصحيح والخطأ في العبارات التَّالية:

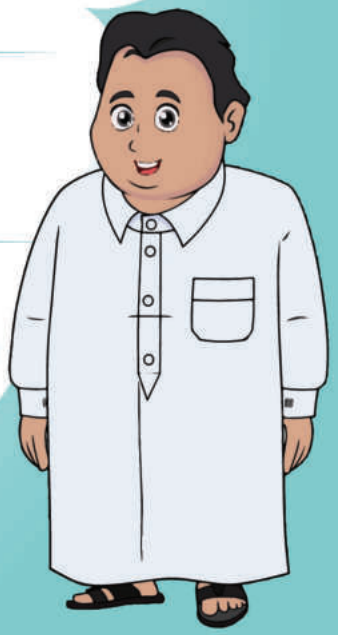
توجيه

اقْرأ الجمل الواردة أدناه بتمعُّن، وفكِّر بدقَّة فيما إذا كانت الجمل صحيحة أم خاطئة، وأدناه مثال محلول.

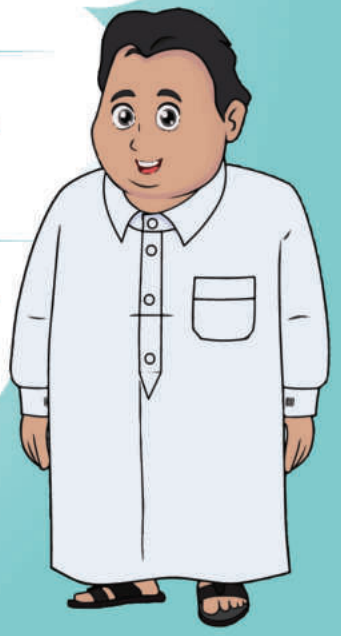
1	يَستَغِلّ مُجْرِمو الاحتيال عبر الإنترنت ثقة النَّاس من أجل سرقة أموالهم وبياناتهم.	صحيح
2	يَدْرُس المُجْرِم الإلكترونيّ الضَّحيَّة لمعرفة نقاط ضعفها؛ لكسب الثِّقة قبل القيام بجريمته.	
3	الشَّركات الكبرى لا تتعرَّض أبدًا لأيٍّ من جرائم الاحتيال عبر الإنترنت.	
4	لا يمكن لجرائم الاحتيال عبر الإنترنت أن تدخل في أيّ مجالات أخرى غير سرقة الأموال والبيانات.	
5	لا يسعى مُجْرِمو الاحتيال عبر الإنترنت إلَّا إلى الحصول على الأموال فقط.	

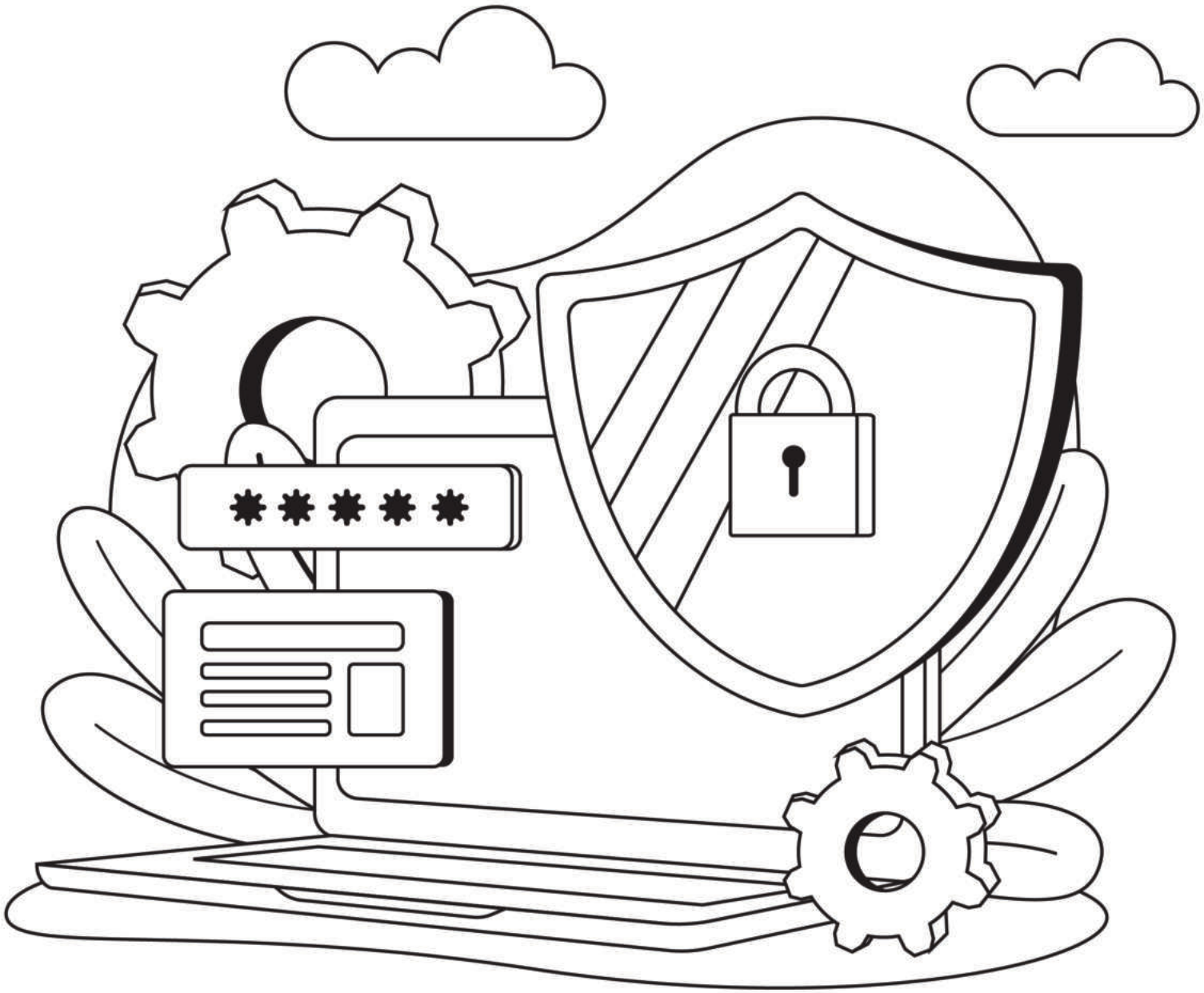


6	استخدام التَّطبيقات غير القانونيَّة يُساعِد مرتكبي جرائم الاحتيال عبر الإنترنت.
7	يمكن تحميل التَّطبيقات من أيّ موقع على الإنترنت دون خوف.
8	لا بأس من مشاركة البيانات والمعلومات السِّرِّيَّة مع الآخرين عبر الهاتف.
9	لا تحتاج إلى استخدام برامج مكافحة الفيروسات.
10	استَخْدِم الأرقام من 1 إلى 8 ككلمة مرور لحساباتك وأجهزتك.



11	يمكنك التَّسوُّق من أيّ متجرٍ إلكترونيٍّ ومشاركة بيانات بطاقاتك البنكيَّة دون خوف.
12	لا يمكن الاحتيال باسم المؤسَّسات الخيريَّة أو التَّطوُّعيَّة.
13	التِّجارة الإلكترونيَّة من أكثر الأهداف التي يستَهدِفها مُجْرمو الاحتيال عبر الإنترنت.
14	الرَّوابط الخبيثة التي تَضْغَط عليها دون وَعْيٍ قد تتسبَّب في سرقة بياناتك وحساباتك.
15	لا يمكن لفيروسات الفدية أن تتسبَّب في أيّ ضررٍ لأجهزتك أو بياناتك.



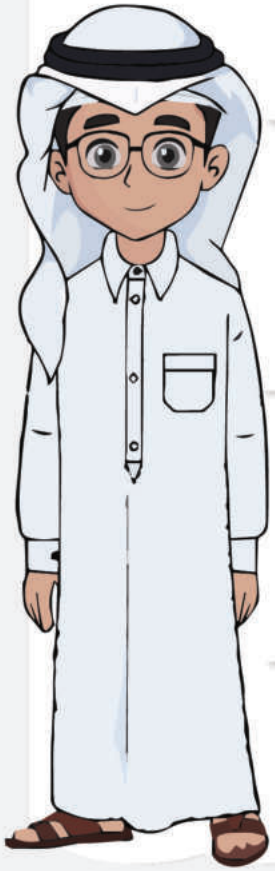


التَّمرين الثَّالث

أكْمِل الجمل التَّالية:

توجيه

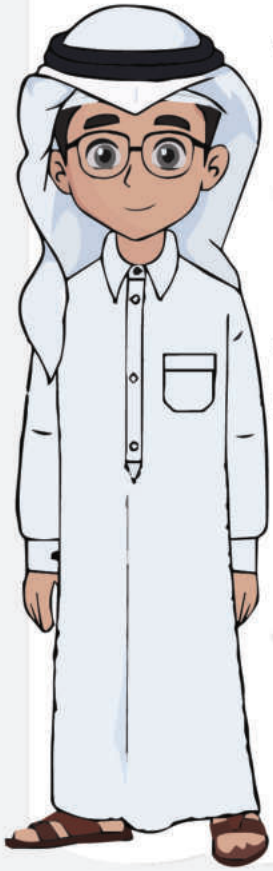
اقرأ الجمل الواردة أدناه بتمعُّن، وحدِّد الكلمات اللَّازمة لملء الفراغ ليُصبِح للجملة معنًى مفيدٌ، وأدناه مثال محلول.



1. ....**البَصْمة الرَّقميَّة**....هي الظِّلّ الرَّقميّ، وتعني أثر البيانات التي تتركها عند استخدام الإنترنت.

2. تشمل البصمة الإلكترونيَّة زيارات .....، ورسائل .....، والمعلومات التي تَبْحَث عنها.

3. البصمة الرَّقميَّة ..... وهي حين تُشارِك معلومات عن نفسك عن عَمْدٍ من خلال المُشارَكة في مواقع ..... أو المنتديات.

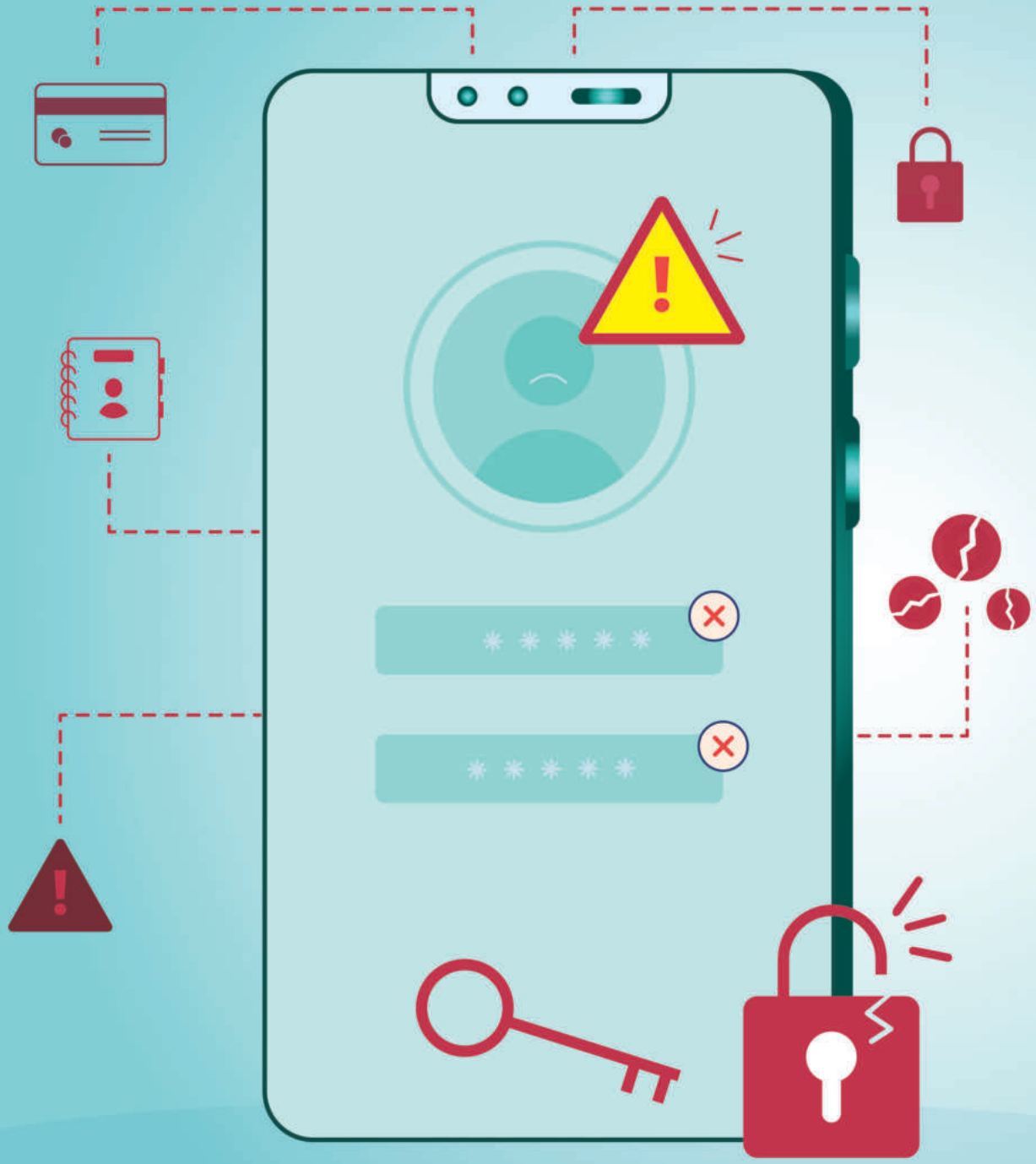


4

البصمة الرَّقميَّة ..... تحدث من خلال جَمْع المعلومات حول المُستخدِم دون أن يُدرِك ذلك، سواءٌ من زياراته للمواقع أو المعلومات التي يبحث عنها ويَستخدِم فيها عنوان الـ ..... الخاصّ به.

5

للبصمة الرَّقميَّة أهميَّة كبيرة، خاصَّةً أنَّها تُعَدّ بيانات ..... ، وتُحدِّد سُمعَة ..... ، وتلجأ بعض جهات العمل إلى تَتَبُّع ..... الرَّقميَّة الخاصَّة بالموظَّفين المُحتمَلين، ويمكن أن يُساء تفسير بعض الكلمات أو ..... التي تُشارِكها عبر الإنترنت، ممَّا يؤثِّر على سُمعَتك أو ..... الرَّقميَّة.



هل تعلم؟

استخدام كلمة مرور قويَّة وتغييرها بين الحين والآخر يحميك من الاحتيال عبر الإنترنت.

التَّمرين الرَّابع

كيف يمكنك حماية نفسك من **الاحتيال عبر الإنترنت؟**

ضَعْ علامة «✓» أو «✗»

توجيه

اقْرأ الجمل الواردة بتمعُّن، وفكِّر بدقَّة فيما إذا كانت الجمل صحيحة أم خاطئة، ويوجد مثال محلول.

1. تحميل تطبيقات موثوقة من المتاجِر الرَّسميَّة.	✓
2. استخدام نُسَخ معدَّلة ومُسَرَّبة من التَّطبيقات الخاصَّة بالهواتف المحمولة.	
3. استخدام برامج مكافحة الفيروسات وجدران الحماية.	
4. مشاركة البيانات الشَّخصيَّة عبر مِنصَّات التَّواصل الاجتماعيّ.	
5. مشاركة البيانات عبر الاتِّصالات الهاتفيَّة.	
6. التَّسوُّق من المتاجِر الموثوقة فقط.	
7. تجنَّب مشاركة بيانات البطاقات البنكيَّة عبر المواقع الإلكترونيَّة.	
8. لا بأس بالدُّخول إلى الرَّوابط مجهولة المصدر.	
9. احْذَر الاستعانة بأطراف مجهولة في أثناء عمليَّات تحويل الأموال أو استلامها.	
10. اخْتَر كلمة مرور مُعقَّدة مُكَوَّنة من حروف كبيرة وصغيرة وأرقام وبعض الرُّموز.	

التَّمرين الـخـامس

حدِّد الخطأ الذي وقع فيه كلّ ضحيَّة من ضحايا جرائم **الاحـتـيـال عبر الإنترنت** التَّالية:

وَصَلَ إلى حمد بريد إلكترونيّ بهدية "IPhone 14"، فقام على الفور بفتح الرَّابط الموجود أمامه، ولكنَّه لم يَصِل إلى شيء.

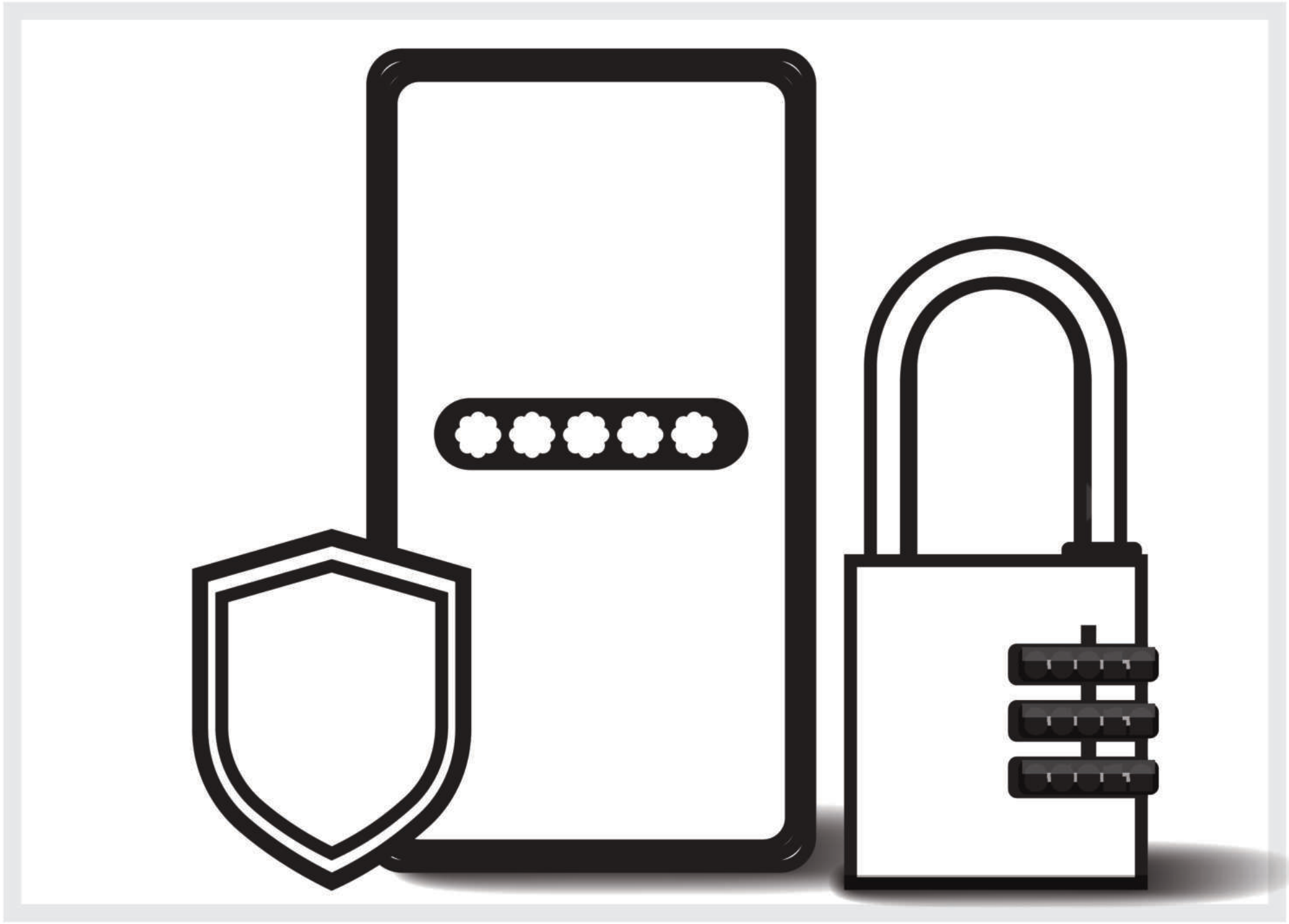
وَصَلَتْ رسالة من رقمٍ دوليٍّ إلى هاتف "هالة" تَطْلُب منها إرسال كلمة الـمرور الخاصَّة بحسابها على Facebook، وفور إرسالـها لم تتمكَّن من الدُّخول إلى حسابها من جديد.

تَواصَل أحد موظَّفي خدمة العملاء في البنك مع "عبد الله" ليتأكَّد من صِحَّة بيانات بطاقته وحسابه البنكيّ، وبعدها وَجَدَ "عبد الله" رسالة تُخْبِره بسحب 50 ألف ريال من حسابه.

شاهـدت "منى" إعـلانًا مُموَّلًا على Facebook لـجمعيَّة تَجْمَعُ التَّبرُّعـات للّاجئين في بعض الدُّول، فأرسلت إليهم مبلغًا من المال، وحيـن حَـاوَلَـت التَّواصل معهم للتَّأكُّد من وصول هذا المبلغ، لم تَجِدْ أيّ شخص يَرُدّ عليها.

هل تعلم؟

تسجيل الدُّخول إلى بعض مواقع الإنترنت باستخدام بيانات حسابك على Facebook قد يُعرِّضك للاحتيال عبر الإنترنت.



تَتَكوَّن البصمة الرَّقميَّة من خلال

1. التَّسوُّق عبر الإنترنت.
2. التَّسجيل لإنشاء حساب على موقع ويب معيَّن.
3. تنزيل التَّطبيقات واستخدامها.
4. استخدام وسائل التَّواصل الاجتماعيّ على الأجهزة الخاصَّة بك.
5. تسجيل الدُّخول إلى مواقع الويب الأخرى باستخدام بيانات Facebook.
6. التَّواصل مع الأصدقاء وجهات الاتِّصال عبر الإنترنت.
7. مشاركة المعلومات والبيانات والصُّور مع معارفك.

طُرق حماية البصمة الرَّقميَّة

1. التَّحَقُّق من المعلومات الخاصَّة بنا عبر استخدام محرِّكات البحث.
2. إزالة المعلومات الشَّخصيَّة من المواقع الإلكترونيَّة.
3. تقييد كمِّيَّة البيانات التي يتمّ مشاركتها عبر الإنترنت.
4. التَّحقُّق من إعدادات الخصوصيَّة بمواقع التَّواصل الاجتماعيّ.
5. تجنُّب المواقع غير الآمنة.
6. الحَذَر عند استخدام شبكةِ Wi-Fi عامَّةٍ.
7. حَذْفُ الحسابات القديمة الخاصَّة بنا على الإنترنت.
8. إنشاء كلمات مرور قويَّة.
9. عدم تسجيل الدُّخول إلى مواقع الإنترنت باستخدام بيانات Facebook.
10. تحديث البرامج والتَّطبيقات باستمرار.
11. تعيين كلمة مرور للهاتف المحمول.
12. التَّحَرُّك بسرعة بعد انتهاك البيانات.

إرشادات الحماية من الاحتيال عبر الإنترنت

1. تحميل التَّطبيقات من المتاجر المعروفة.
2. تحديث نظام الهاتف.
3. تجنُّب الرَّوابط مجهولة المصدر.
4. الحذر من المعاملات التي تتضمَّن أطرافًا مجهولة، مثل تحويلات الأموال.
5. الاستعانة ببرامج مكافحة الفيروسات.
6. استخدام كلمات مرور قويَّة، وتغييرها بين الحين والآخر.
7. عدم التَّسوُّق عبر المواقع المجهولة.


CREDIT
CARD
234 5678 9101 2134
000 00/00
* * * * *

انْتَبِه!

أمان المعلومات

مجموعة من الإجراءات والأدوات الأمنيَّة التي تَحْمِي على نطاق واسع المعلومات الحسَّاسة من سوء الاستخدام أو الوصول غير المُصَرَّح به أو التَّعطيل أو الإتلاف.


المسابقات

اختر الإجابة الصَّحيحة

1. **أيّ ممَّا يلي يُعَدّ من الأمثلة على البصمة الرَّقميَّة النَّشطة؟**

- [ ] المنشورات على مِنصَّات التَّواصل الاجتماعيّ.
- [ ] التَّطبيقات التي تَستخدِم تحديد الموقع الجغرافيّ.
- [ ] مواقع الويب التي تُثَبِّت ملفَّات الارتباط دون إخطار المُستخدِم.

2. **من أهمّ مصادر المعلومات الشَّخصيَّة روابط التَّعريف الخاصَّة بالتَّطبيقات والمواقع الإلكترونيَّة.**

- [ ] صحيح.
- [ ] خطأ.

3. **تتمّ عمليَّة الاحتيال عبر الإنترنت عادةً عند زيارة الأفراد للمواقع الإلكترونيَّة أو غرف الدَّردشة أو المتاجِر الإلكترونيَّة أو المدوَّنات أو التَّطبيقات.**

- [ ] صحيح.
- [ ] خطأ.

4. **الخِداع أو الغِشّ المعلوماتيّ من المفاهيم المُرْتَبِطة بمفهوم الاحتيال عبر الإنترنت، ويُطلَق عليه "الاحتيال المعلوماتيّ".**

- [ ] صحيح.
- [ ] خطأ.

5. **النَّصْب عبر الإنترنت هو الاستيلاء على مال الآخرين بواسطة الخِداع، من خلال استخدام أجهزة الحاسوب والهواتف الذكيّة والأجهزة اللّوحيّة.**

- [ ] صحيح.
- [ ] خطأ.

6. **من أسباب الاحتيال عبر الإنترنت:**

- [ ] عدم اتباع قواعد التَّصفح الآمن للإنترنت.
- [ ] التَّعامل مع المتاجِر الإلكترونيَّة غير الموثوقة.
- [ ] استغلال مشاعر التَّعاطف.
- [ ] جميع ما سبق.

7. **رسائل البريد الإلكترونيّ التي تَتَضَمَّن روابط مسابقات أو جوائز ماليَّة وعينيَّة مغرية من أشكال الاحتيال عبر الإنترنت.**

- ☐ صحيح.
- ☐ خطأ.

8. **الثَّغرة الأمنيَّة هو مصطلح يُطلَق على مناطق القُوَّة في أنظمة تشغيل الحاسوب والبرامج.**

- ☐ صحيح.
- ☐ خطأ.

9. **لا تُمَثِّل الثَّغرات غير المكتشفة Zero-Day تهديدًا للأمن السّيبرانيّ.**

- ☐ صحيح.
- ☐ خطأ.

10. **خطوة "إنشاء رمز الاستغلال" تقع ضِمن آليَّة عمل هجوم الثَّغرات غير المكتشفة Zero-Day.**

- ☐ صحيح.
- ☐ خطأ.

11. **كلمة "سرقة" في عالم الإنترنت يُطلَق عليها ....**

- ☐ انتهاك البيانات.
- ☐ تَسَرُّب البيانات.
- ☐ جميع ما سبق.

12. **يمكن استخدام ..... لتَتَبُّع أنشطة أيّ شخص عبر الإنترنت.**

- ☐ بصمة الوجه.
- ☐ بصمة اليدّ.
- ☐ البصمة الرَّقميَّة.

قُم بتوصيل الجمل من العمود (أ) بما يُناسبها من العمود (ب)

العمود (أ)	العمود (ب)
من أدوات الاحتيال عبر الإنترنت	سرقة البيانات.
رسائل البريد الإلكترونيّ المُزيّفة	الاحتيال عبر الإنترنت.
من أمثلة جرائم الاحتيال عبر الإنترنت	أمان المعلومات.
إحدى الثّغرات الأمنيّة التي تُصيب البرمجيّات	سرقة العُملات الرّقميّة، مثل البيتكوين.
مجموعة من الإجراءات والأدوات الأمنيّة التي تَحْمِي المعلومات الحسّاسة من سوء الاستخدام	استغلال حالات الطّوارئ، مثل جائحة كورونا.
سرقة معلومات رقميّة مُخزّنة على أجهزة الحاسوب أو الهواتف بغرض انتهاك الخصوصيّة	أحد أشكال الاحتيال عبر الإنترنت.
مرادف كلمة سرقة في مجال الإنترنت	الثّغرات غير المُكْتَشفَة Zero-Day.

ضَع الكلمة أو العبارة المرادفة للجُمَل التَّالية

هجوم تَتَعرَّض له يُعطِّل حساباتنا على الإنترنت، ومقابل إعادةِ استخدامها علينا دَفْع مبلغٍ ماليٍّ. .....

رسائل بجوائز ماليَّة وهدايا مُزيَّفة تَصِل إلينا عبر البريد الإلكترونيّ أو Messenger، وهَدَفُها خِداعنا وسرقة بياناتنا. .....

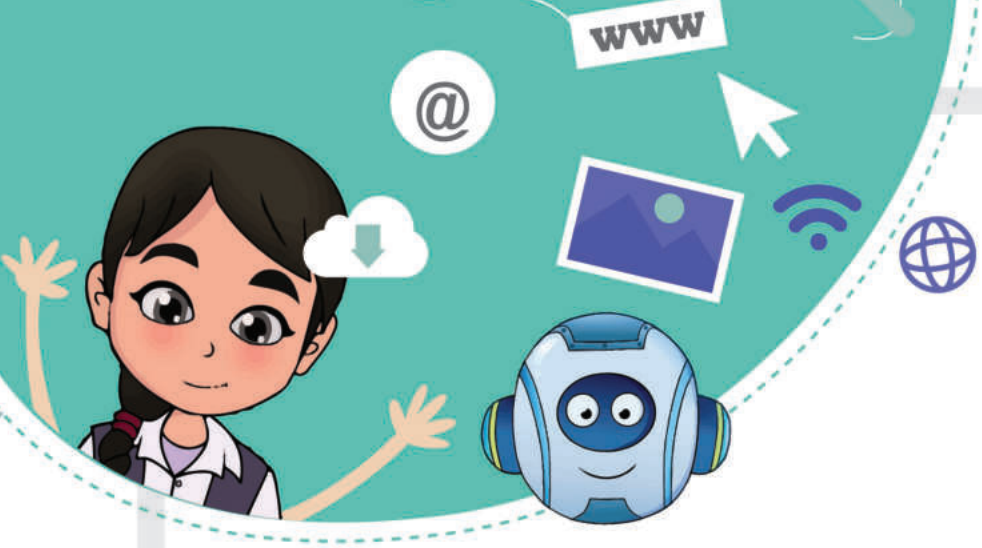
نقاط ضعف تتسبَّب في خَرْق أجهزتنا، سواءٌ الحاسوب أو الهاتف الذَّكيّ أو الأجهزة اللَّوحية، وتُعَرِّضنا للخطر. .....

أدوات تَحْمِي معلوماتنا الحسَّاسة من الوصول إليها وتعطيلها أو إتلافها. .....

سرقة من نوع خاصّ تَسْتَهْدِف بياناتنا الشَّخصيَّة على الإنترنت ويُعاقِب القانون فاعِلها. .....

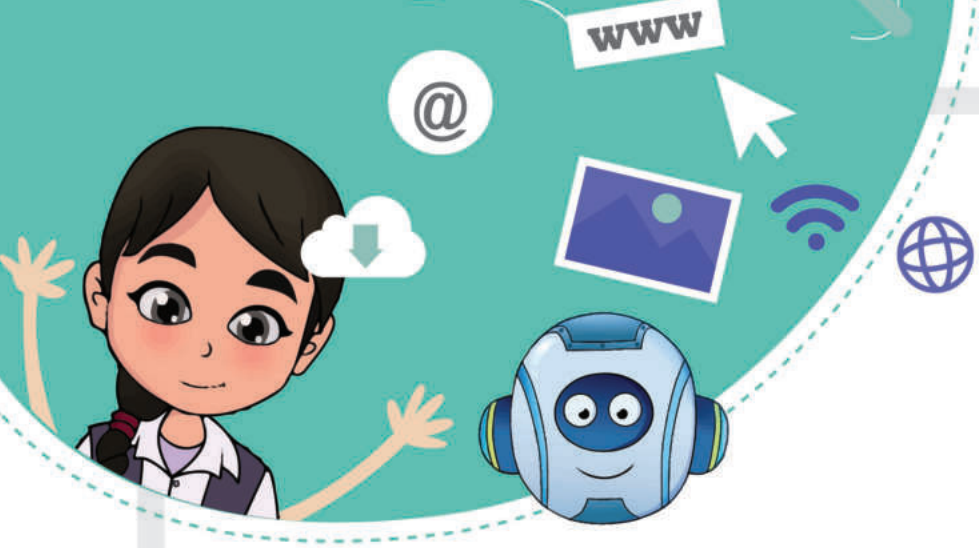
آثار على الإنترنت يَستخدِمها المُهاجِمون لاستغلال ما بها من معلومات وبيانات حسَّاسة لخِداعنا وكذلك خداع الآخرين. .....

تَتَكوَّن من 12 حرفًا ورمزًا ورقمًا، وهَدَفُها حمايتنا على الإنترنت. .....



أُكْمِل الجمل التَّالية بالإجابات الصَّحيحة:

1. البصمات الرَّقميَّة ..... يُقصَد بها مُشارَكة المُستخدِم معلومات عن نفسه عمدًا.
2. البصمة الرَّقميَّة ..... يُقصَد بها جَمْع معلومات حول المُستخدِم دون أن يُدرك أنّ هذا يَحْدُث.
3. يستطيع مُجْرمو الإنترنت استغلال ..... لأغراضٍ مثل سرقة الهوية عبر الإنترنت.
4. من بين الطُّرق التي يُضِيف بها المستخدمون إلى بصمتهم الرَّقميَّة تنزيل .....
5. من طُرق حماية البصمة الرَّقميَّة تقييد .....



6 التَّحَقُّق من إعدادات الخصوصيَّة من طُرق حماية .....

7 من إرشادات الحماية من الاحتيال عبر الإنترنت تجنُّب الرَّوابط .....

8 يُفَضَّل أن تُستخدَم كلمات مرور مُكَوَّنة من ..... للحماية من الاحتيال عبر الإنترنت.

9 في حال التَّعرُّض لجريمة الاحتيال عبر الإنترنت نلجأ إلى إبلاغ .....

10 إذا كانت شاشتك تمتلئ بشَكلٍ مفاجئٍ بالنَّوافذ المنبثقة، فيجب .....

انْتَبِه!

البَصْمَة الرَّقميَّة

تُشير إلى أثر البيانات والمعلومات التي تتركها عند استخدام الإنترنت، وهي تشمل مواقع الويب التي تزورها، ورسائل البريد الإلكترونيّ التي تُرسلها وتستقبلها، والمعلومات التي تُقَدِّمها عبر الإنترنت.

وتُحدِّد **البصمة الرَّقميَّة** سُمْعَة الأشخاص على الإنترنت كما يَحْدُث في الحياة العاديَّة.

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجب يقوم به الطَّالب بمفرده أو بالاشتراك مع زميل أو أكثر، ويقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

يَتقمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوْجِيهاتٍ عامَّةً لزملائه أو أَهْله يُوضِّح لهم فيها الإجراءات المطلوبة للوقاية من مخاطر التَّزوير والاحتيال عبر الإنترنت.

كتابة قِصَّة قصيرة تَدَور أحداثها حول طالبٍ تَعَرَّض لمحاولة احتيالٍ عبر الإنترنت، وكيف تَصَرَّف حِيَال هذا الموقف.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency