



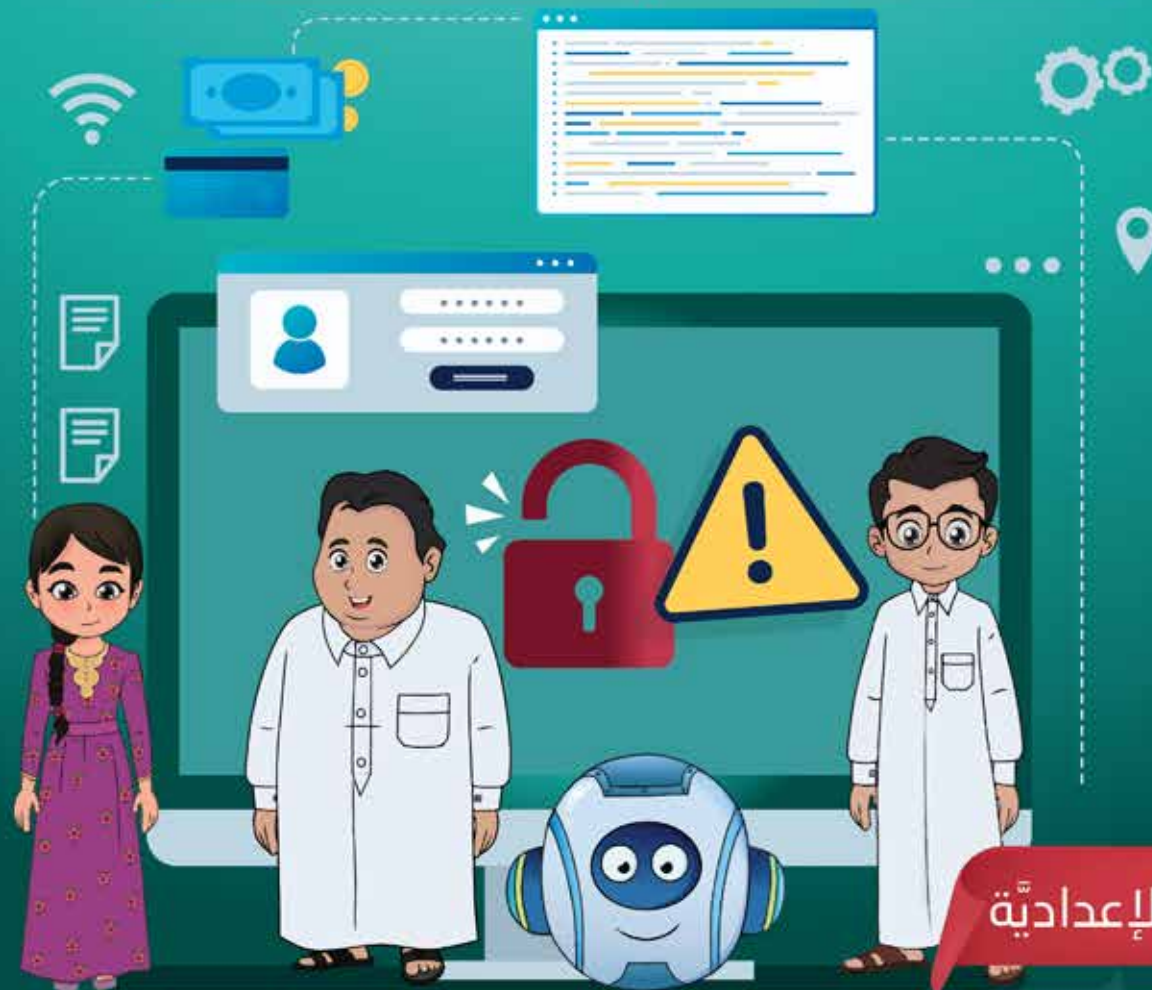
CyberEco

معا لدعم السلامة الرقمية
Together to support digital safety

التزوير والاحتيال الإلكتروني

تمارين وتدريبات الطالب

الحقيبة التدريبية



المرحلة الإعدادية



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

التّزوير والاحتياال عبر الإنترنت

تَمَارِين وَتَدْرِيبَات الطَّالِب

المرحلة الإعدادية

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافة حقوق الملكية الفكرية التي تشمل حق المؤلف وحقوق التأليف والنشر والطباعة، كلها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر. وعليه، فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي أجزاء من هذه المادة، أو الاقتباس منها، أو نسخ أي جزء منها، أو نقلها كلياً أو جزئياً في أي شكل وبأي وسيلة، سواءً بطرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نظم تخزين المعلومات واسترجاعها سواءً من الأنظمة الحالية أو المبتكرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذن خطي منها.

ومن يخالف ذلك يُعرض نفسه للمساءلة القانونية.

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدارة التميز السيبراني الوطني، الوكالة الوطنية للأمن السيبراني.

للاستفسار عن المبادرة أو البرنامج؛ يمكن التواصل عن طريق المواقع الإلكترونية أو الأرقام الهاتفية التالية:



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

عزيزي الطالب

هذا الكُتَيْب خاص بك، ولا بُدَّ أن يكون معك عند حضورك جلسات التدريب، وسيقوم مُدَرِّبك بإرشادك إلى كيفية استخدامه، ويحتوي هذا الكُتَيْب على مجموعة من التمارين الممتعة والمفيدة، والتي ستقوم بالإجابة عنها إمَّا خلال الصَّف وإمَّا في منزلك. كما يحتوي الكُتَيْب على مجموعة من المسابقات والبطاقات التَّعليميَّة، والمعلومات العامَّة، والتي ستجد فيها فائدة ومتعة، وسيرشدك المُدَرِّب إلى كيفية التَّعامل مع هذه المسابقات، كما سنزوِّدك في مطلع كلِّ تمرين أو مسابقة بتوجيهات عامَّة لكيفية الإجابة.

السادة أولياء أمور الطلبة

كل التمرينات والتدريبات الموجودة في الكتيب، ستكون مرفقة بتوجيهات عامة لكيفية الإجابة عنها، أما المسابقات التدريبية فالمدرّب هو من سيُقدّم للطالب توجيهات حلّها، كما أنّ الكتيب يحتوي على بعض التدريبات والتمارين اللاصفية، وهذه التمارين سيقوم بالإجابة عنها بالمنزل، وهي الأخرى ستكون مرفقة بتوجيهات للحلّ.

يُرجى منكم الإشراف غير المباشر على الطالب خلال تعامله مع الكتاب، وفي حال توجّه الطالب إليكم بسؤال أو استفسار حول أحد التمارين أو التدريبات، فيُرجى قراءة التوجيهات الخاصة بكل تمرين، وتقديم العون للطالب في ضوء هذه التوجيهات.

هذا الكتيب خاصّ بالطالب، وسيرافقه خلال التدريب الذي سيتلقّاه في المدرسة، وهو يحتوي على مجموعة من التمارين والتدريبات والمسابقات والبطاقات التدريبية، والتي تتمحور جميعها حول المفاهيم ذات الصلة بالتزوير والاحتيال عبر الإنترنت، وكيفية الوقاية من هذه المخاطر.

الهدف من هذا الكتيب وما يحتوي عليه من تدريبات وأنشطة ذهنية تكريس وترسيخ المعلومات التي تلقّاها الطالب خلال محاضرة التدريب؛ وذلك لتحقيق هدف رئيسي، يتمثل في تعزيز قدرة الطالب على استخدام الإنترنت والتكنولوجيا بفاعلية وأمان، وتدريبه على كيفية التعامل مع مخاطر الاحتيال عبر الإنترنت وكيفية عدم الوقوع ضحية له.

انتبه!

الاحتيال عبر الإنترنت

نوع من أنواع الخداع والحيل التي تتم على شبكة الإنترنت، وغالبًا ما تحدث هذه الجرائم في غرف الدردشة أو عبر البريد الإلكتروني أو على المنتديات أو مواقع الإنترنت (الويب)، والهدف من هذه الجرائم هو الاحتيال على العملاء والمستخدمين عن طريق سرقة الأموال والمعلومات الشخصية المهمة وغيرها من الأغراض الأخرى.



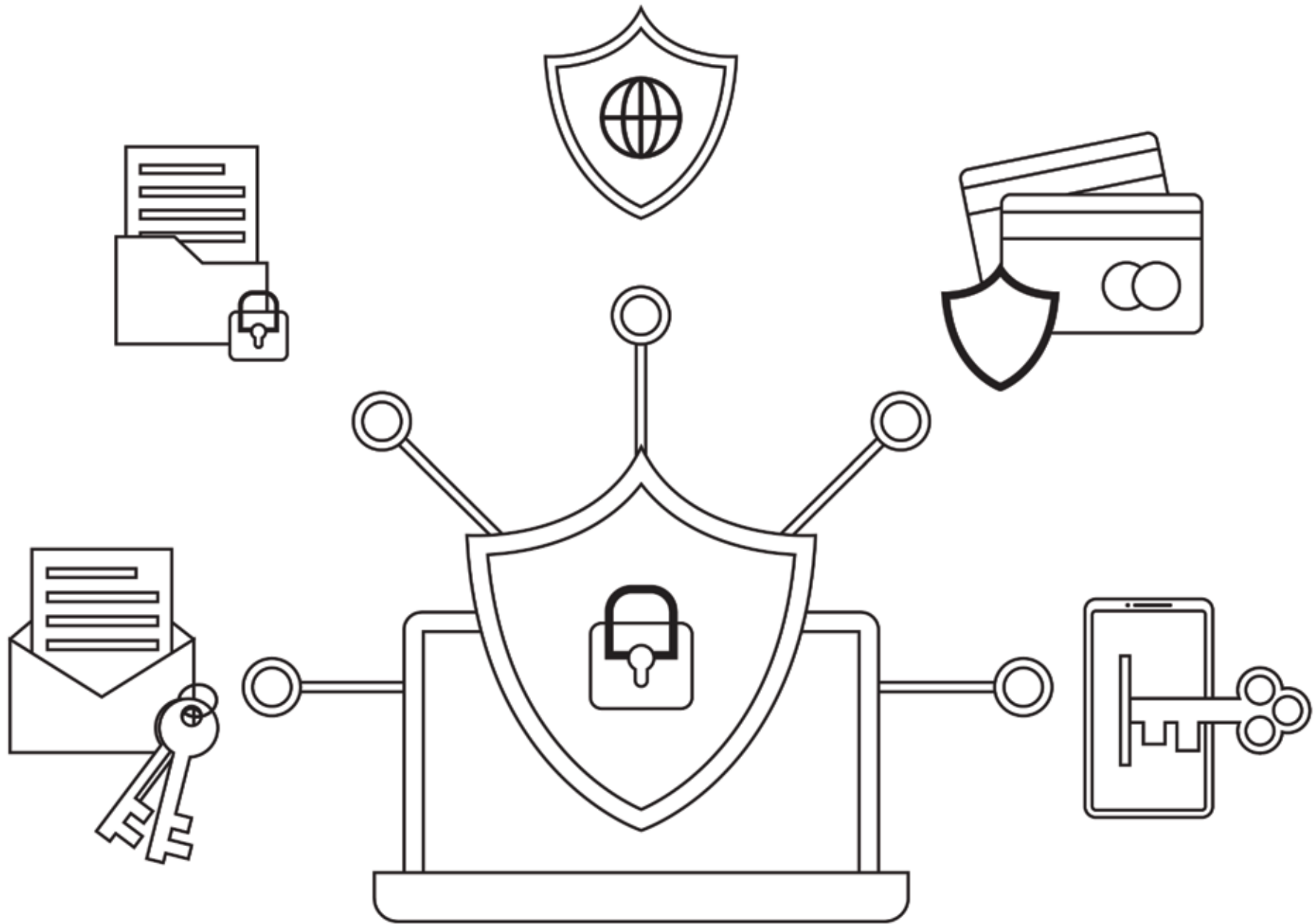


أولاً: التمارين الصفيّة



هل تعلم؟

غالبية الجوائز والهدايا التي تأتي عن طريق الإنترنت دون سبب تكون بدايةً لعملية احتيال عبر الإنترنت.



التمرين الأول

ضع علامة (✓) بجانب العبارة الصحيحة، أو علامة (X) بجانب العبارة الخاطئة:



جريمة الاحتيال عبر الإنترنت هي تلاعب متعمّد في المعلومات والبيانات الموجودة على الحاسوب والأجهزة الذكية.



جريمة الاحتيال عبر الإنترنت هي الدّخول المُصرّح به من أجل الحصول على معلومات وبيانات موجودة على الحاسب الآلي.



يَقَدّ الدّخول على الأجهزة أو الأنظمة من أجل الحصول على ربح غير مشروع أو إلحاق ضررٍ ما بها من أنواع جرائم الاحتيال عبر الإنترنت.



تُساعد التّقنيّة الحديثة مُرتكبي جرائم الاحتيال عبر الإنترنت على ارتكاب الجرائم على النّطاق المحليّ فقط.

1

2

3

4

توجيه

اقرأ الجمل الواردة أدناه بتمعّن، ثم حدّد ما إذا كانت الجملة صحيحة أم خاطئة، وأدناه مثال محلول.





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



6 الاحتيال المعلوماتي هو الفِش والخداع المعلوماتي من خلال التَّلاعب بأنظمة المُعالجة الآليَّة للمعلومات دون وجه حق، من أجل الحصول على الخدمات أو الأموال أو الأصول.



7 النَّصب عبر الإنترنت هو الحصول على الأموال بطرق غير مشروعة من خارج الدَّولة فقط.



8 يَستخدم الجُناة في الاحتيال عبر الإنترنت التَّقنيَّات بطريقة مشروعة ودون أيِّ تلاعب.

5

6

7

8

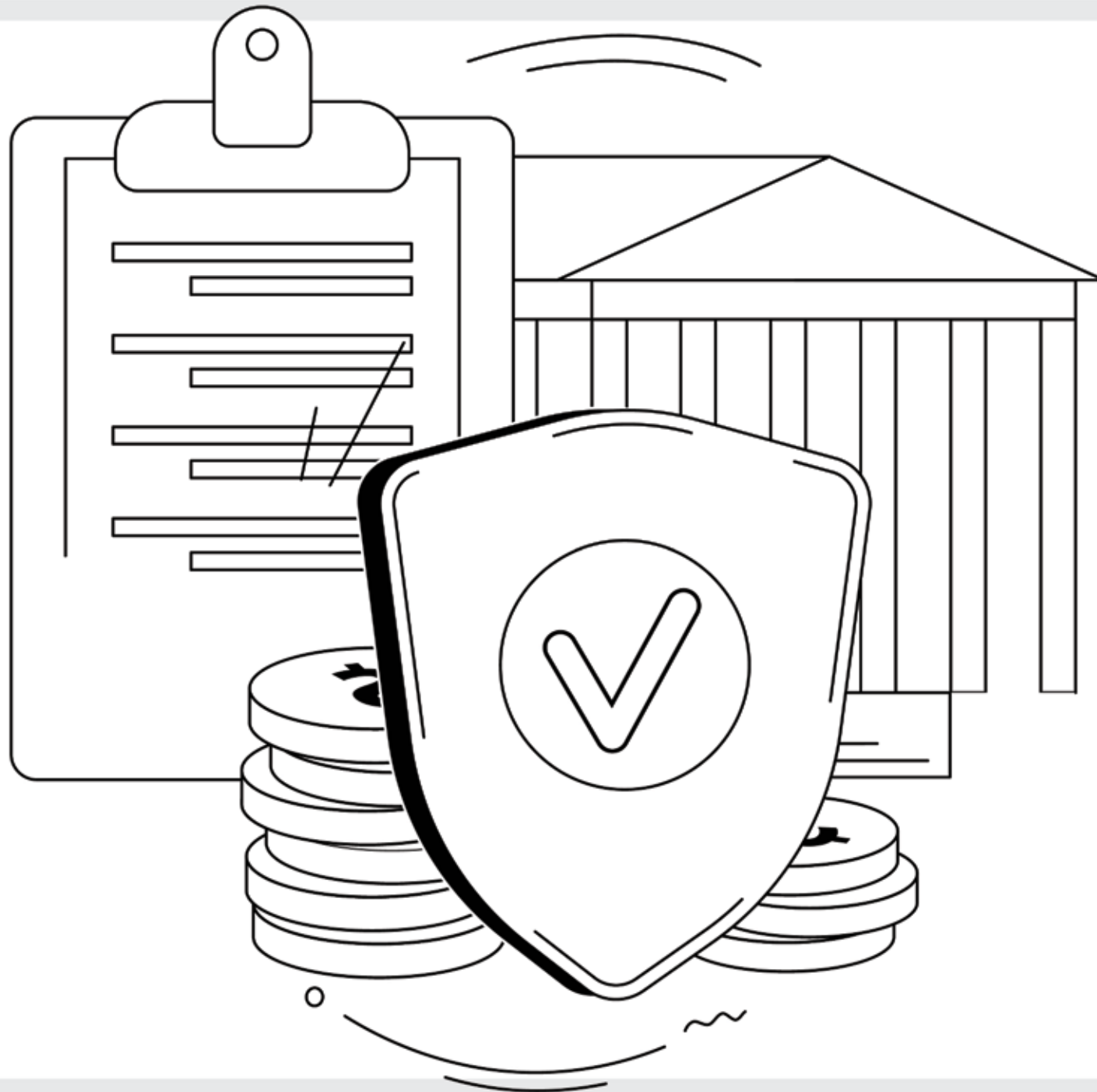


انتبه!

النصب عبر الإنترنت

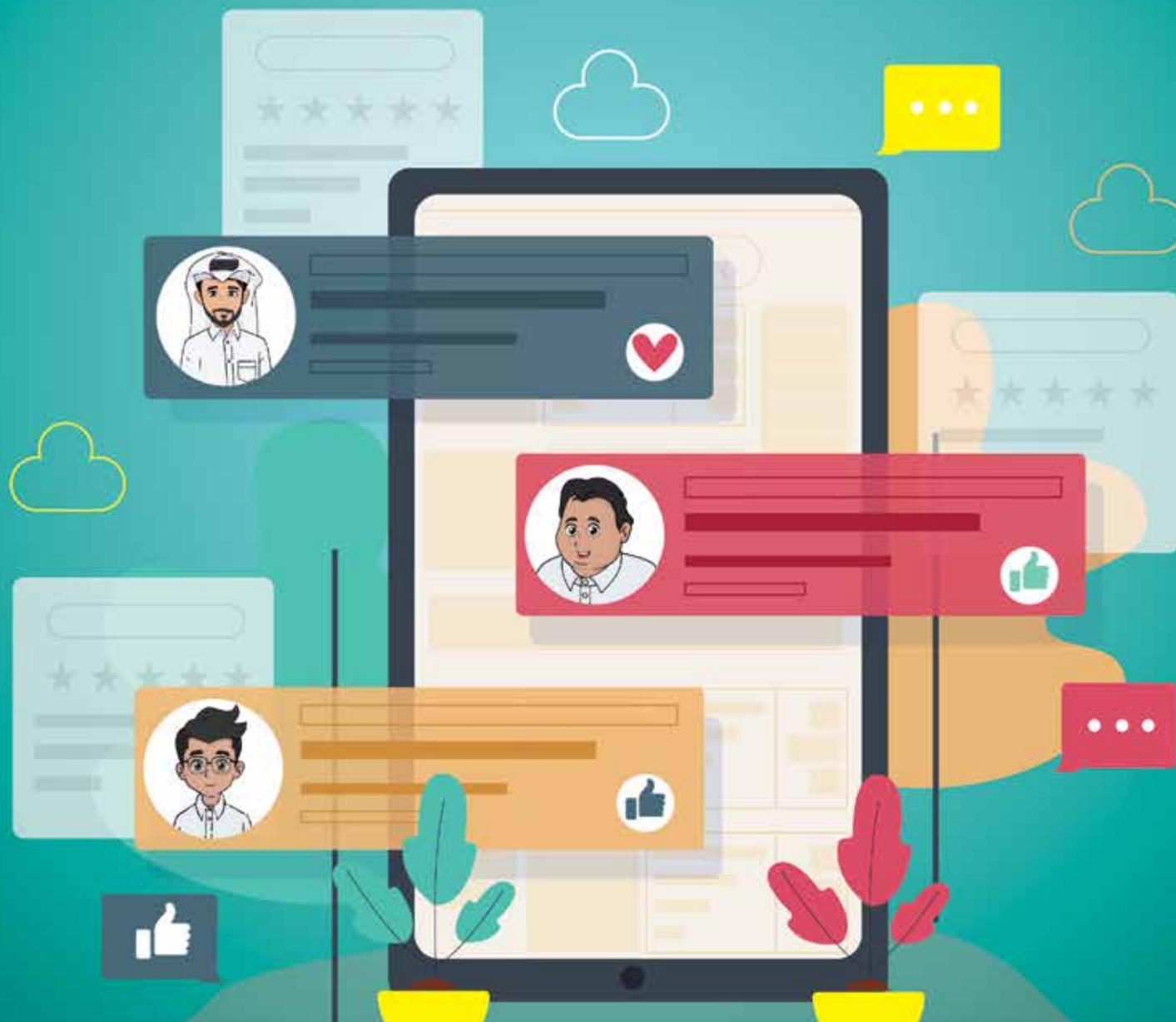
الاستيلاء على مال الآخرين بوسيلةٍ يشوبها الخداع، ما يتسبب في تسلم هذا المال عن طريق أجهزة الحاسوب والأجهزة الذكية.





هل تعلم؟

تُحدّد البصمة الرقمية سُمعة الأشخاص على الإنترنت كما يَحْدُث في الحياة العادية.



التّمرين الثاني

صل المُضطلّحات والعبارات من العمود (أ)
بما يناسبها من العمود (ب):

توجيه

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

العمود (أ)

- ☐ الاحتيال عبر الرّسائل النّصّية القصيرة
- ☐ الاحتيال عبر الإعلانات
- ☐ فيروسات الفدية
- ☐ الاحتيال بسرقة بطاقات الائتمان
- ☐ الاحتيال الصّوتي
- ☐ احتيال التّسوّق عبر الإنترنت
- ☐ الاحتيال بجمع التّبرّعات
- ☐ الاحتيال على البائع عبر الإنترنت

العمود (ب)

- ☐ نوع من أنواع الاحتيال عبر الإنترنت، حينما يتم تهديد الضّحية بإتلاف البيانات أو دَفْع فدية.
- ☐ يعتمد على خداع الآخرين عبر برامج تغيير الصّوت لإقناع الضّحايا بمشاركة البيانات والمعلومات الشخصية.
- ☐ يتم أثناء تسوّق الضّحية، وبعد دفع قيمة المُنتج لا يصل إليه أيّ شيء، أو ربّما يصل إليه مُنتج خاطئ أو مُقلّد.
- ☐ تُستغلّ فيه أسماء جمعيات خيرية وهمية من أجل الحصول على الأموال عن طريق إثارة تعاطف الآخرين.
- ☐ يتم إرسال رابط من خلال رسالة نصّية، وبمجرّد الضّغط عليها تتم عملية الاحتيال.
- ☐ يتم فيه إيهام البائع بأنّ المشتري قام بالدّفع وبعد إرسال المُنتج لا تُضاف الأموال إلى رصيده.
- ☐ يتم من خلال سرقة بيانات بطاقات الائتمان واستخدامها في شراء المُنتجات عبر الإنترنت.
- ☐ الإعلانات الخبيثة المُحمّلة بالفيروسات، التي تُستخدم في سرقة المعلومات والبيانات.

التمرين الثالث

املأ الفراغات بالكلمات المناسبة:

توجيه

اقرأ الجمل الواردة أدناه بتمعن،
وحدّد الكلمات المناسبة لملء
الفراغ؛ بحيث يصبح للجملة معنى
مفيد، وأدناه مثال محلول.

يُعَدّ الاحتيال لسرقة الهوية أخطر أنواع الاحتيال عبر الإنترنت؛ حيث يقوم المجرم بسرقة **البيانات** الشخصية، مثل الاسم وتاريخ **الميلاد** وعنوان **الإقامة** وتفاصيل الحساب **البنكي** وكافة المعلومات المهمة الأخرى.

تُستخدَم تلك المعلومات في سرقة ويمكن أن يتم استغلال الهوية في فتح بنكية، أو الحصول على بطاقات أو قروض، أو من أجل تسجيل خطوط

يمكن لمجرمي الاحتيال عبر الإنترنت سرقة الشخصية للاستيلاء على البنكية المفتوحة بالفعل للشخص، عن طريق شخصيته.

لا بُدّ أن تتجنّب إعطاء الآخرين أيّ شخصية، كما يجب أن تحذف أيّ مستند أو ملف يحتوي على سرية أو أرقام بطاقات قبل التخلّص منه.

1

2

3

4

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

5

عليك أن تنتبه جيدًا في تعاملاتك مع التجارّة، أو مع الآخرين، سواءً من خلال الهاتف أو أو الإنترنت بشكل عامّ، خاصّة منصات

6

تجنّب فتح أيّ غير الموثوقة، وقم بإلغاء المنبثقة، وتأكد من الشخص الذي تتحدّث إليه عبر الإنترنت.

7

استخدم قويّة على هاتفك وحساباتك الشخصيّة، ولا تشاركها مع الآخرين، ولا تنس الاحتفاظ احتياطيّة لبياناتك، وتجنّب استخدام شبكات العامّة، خاصّة إذا كنت ستفتح أيّ تطبيق له علاقة بمعاملاتك البنكيّة.

8

إذا كنت ترغب في التسوّق فعليك أن تتأكد من الشّقة بهذا المتجر، وأن تقرأ تقييمات الآخرين ومراجعاتهم، ومن الأفضل التّعامل مع المتاجر المشهورة والتي تُعرّف بالأمان.

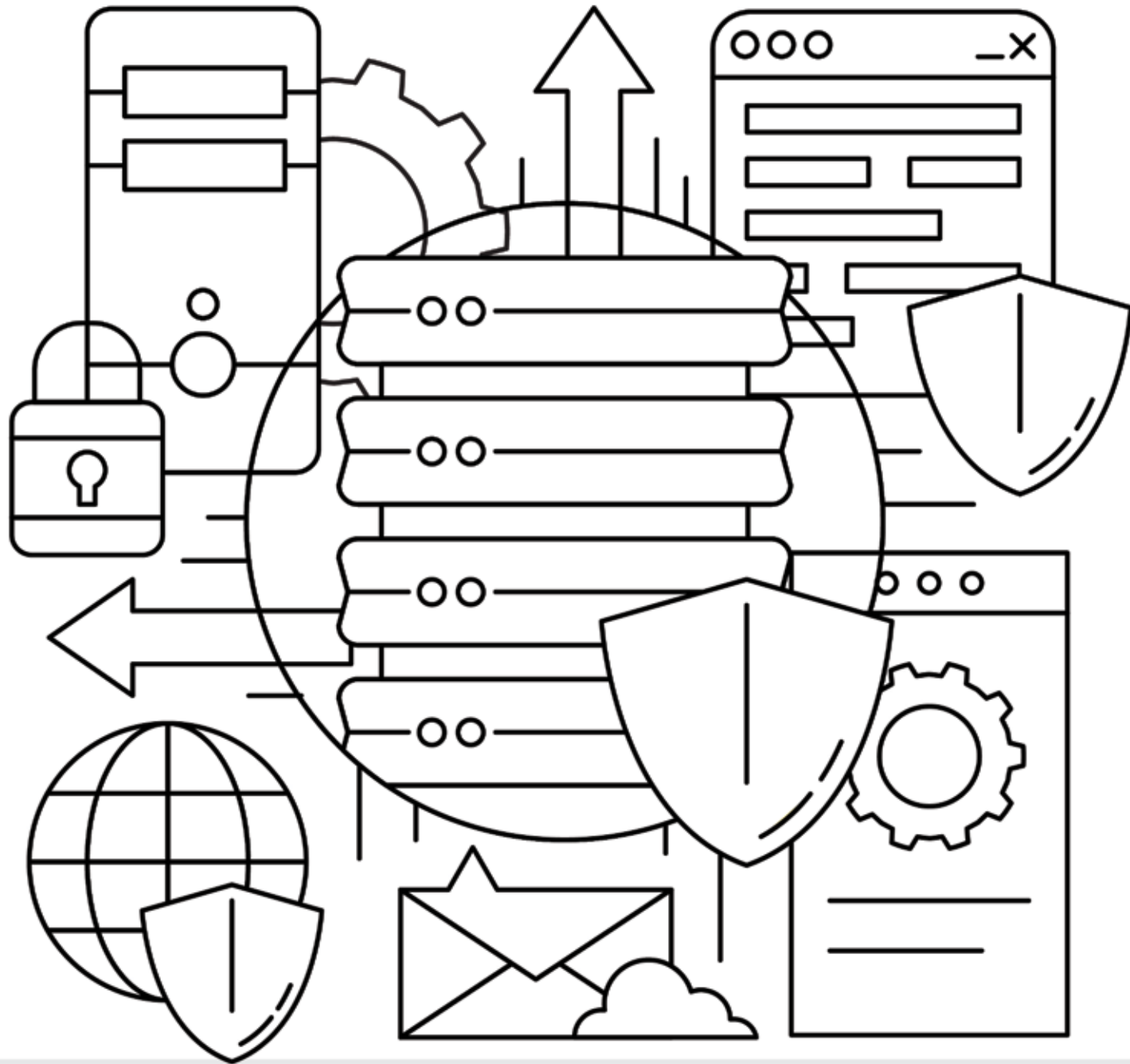
9

انْتَبِه!

الاحتيال المعلوماتي

الخداع أو الفِش المعلوماتي الذي يقوم على التلاعب في نظم المُعالجة الآليّة للمعلومات، بفرض الحصول دون وجه حقّ على خدمات أو أموال أو أصول معيّنة.





التمرين الرابع

توجيه

اقرأ الجمل الواردة في الجدول بتمعن، وحدّد ما إذا كانت الجمل تُعبّر عن معلومات صحيحة أم خاطئة في مجال الحماية من الاحتيال عبر الإنترنت، وفي حال كانت صحيحة ضع بجانبها علامة (✓) ، وإذا كانت خاطئة ضع علامة (X) ، وأدناه مثال محلول.

ضع علامة (✓) أو علامة (X) أمام العبارات التي تُعدّ أساسيّة للحماية من جرائم الاحتيال عبر الإنترنت

✓	1 لا بدّ من استخدام النسخ القانونيّة من التطبيقات البنكيّة.
	2 يمكنك تحميل التطبيقات من أيّ موقع من مواقع الإنترنت.
	3 يجب ألا تذكر بياناتك السريّة والمعلومات الخاصّة بك في أثناء الاتّصالات الهاتفية.
	4 يمكنك أن تضغط على أيّ روابط يُرسلها إليك الأصدقاء، سواءً في الرسائل النصيّة أم عبر البريد الإلكتروني.
	5 الاستعانة بأطراف مجهولة في المعاملات الماليّة قد تُعرّضك لعمليّة نصب أو تبييض أموال.



	استخدام برامج مكافحة الفيروسات عامل أساسي في حمايتك من الاحتيال عبر الإنترنت.	6
	يمكنك تكرار اسمك أو كتابة تاريخ ميلادك كلمة مرور قوية لحساباتك وأجهزتك.	7
	يجب تحري الدقة في أثناء التسوق عبر الإنترنت، ويُفضّل التعامل مع المواقع المعروفة.	8
	يمكنك كتابة بيانات بطاقتك البنكية على أي تطبيق عبر الإنترنت.	9
	تجنّب استخدام النسخ المعدّلة أو المُخرقة من التطبيقات الخاصة بالهواتف الذكية.	10

انتبه!

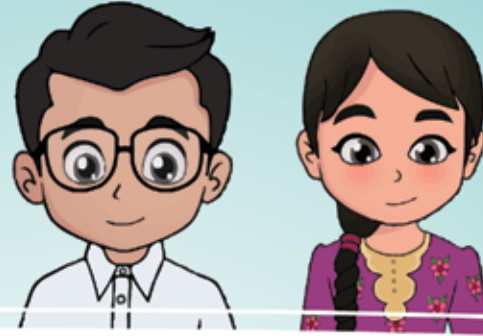
أسباب الوقوع ضحيةً للاحتيال عبر الإنترنت

- قلة وعي الأفراد حول كيفية استخدام وسائل التواصل الاجتماعي ومواقع الإنترنت.
- الدخول إلى مواقع إلكترونية غير آمنة
- نشر الأفراد معلومات شخصية عن أنفسهم عبر مواقع التواصل والإنترنت.
- التعامل مع المتاجر الإلكترونية غير الموثوقة.
- انتحال المتسللين صفة شخصيات معروفة وذات مكانة، مثل شخصيات موظفي الحكومة أو الخبراء أو المسؤولين التنفيذيين أو التقنيين.
- استغلال مشاعر التعاطف، مثل حالات الطوارئ؛ لجذب تعاطف الضحية المُستهدفة عبر الإنترنت.



التمرين الخامس

ضع الكلمة المناسبة
أمام كل جملة:



توجيه

اقرأ الجمل الواردة في الجدول بتمعن، وفكر في كلمة أو عبارة تُعبّر عن معنى الجملة، واكتبها في العمود الثاني، وأدناه مثال محلول.

البصمة الرقمية

1. الأثر الذي تتركه خلفك والمعلومات التي تخلفها بعد كل استخدام للإنترنت.

2. النصب وسرقة البيانات باستخدام تقنيات التكنولوجيا والإنترنت.

3. برامج تساعدك على حماية أجهزتك وصدّ هجمات المحتالين.

4. مجموعة من الحروف والرموز والأرقام التي تستخدم لحماية حساباتك.

5. الاستعانة بوسيط من أجل تحويل الأموال من طرف إلى طرف.

انتبه!

الثغرة الأمنية

مصطلح يُطلق على نقاط ضعف في أنظمة تشغيل الحواسيب والهواتف الذكية والأجهزة اللوحية، والتي يتسلل عبرها المهاجمون إلى داخل نظام التشغيل، ومن ثم يتم التعديل فيه لتدميره نهائياً، أو للتجسس على المعلومات الخاصة بصاحب الحاسوب المُخترق، أو ما يُعرف بجهاز الضحية.







انْتَبِه!

ثغرة Zero-Day

هي ثغرة في برامج الحاسوب يمكن استغلالها من قبل المتسللين، وتؤدي هذه الثغرة الأمنية إلى خرق شديد الخطورة على الأمن السيبراني.

التَّمرين الأول

استخرج الكلمات
التَّالية من الجدول:

توجيه

اقرأ الكلمات الواردة أدناه بتمعُّن، وابحث في الجدول عن حروف متتالية تُشكِّل هذه الكلمات، وأدناه مثال عن كلمة "النَّصَب" وكيف تمَّ إيجاد أحرف الكلمة في الجدول:

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

الاحتِيال - ~~النَّصَب~~ - التَّلَاعِب - بَيانات - الأوامر - التَّقْنِيَّة - الضَّرر

جَريمة - مَجْرَم - خِداع - غِش - إفلاس - حَقِّق

التمرين الثاني

حدّد الصّحيح والخطأ في العبارات التّالية:

توجيه

اقرأ الجمل الواردة أدناه بتمعّن، وفكّر بدقّة فيما إذا كانت الجمل صحيحة أم خاطئة، وأدناه مثال محلّول.

صحيح

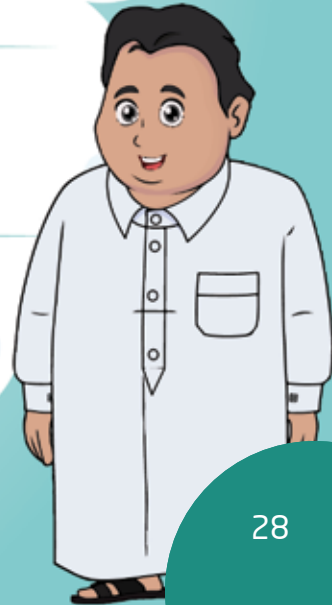
1 يَسْتَفِلُّ مُجْرِمُو الاحتيال عبر الإنترنت ثقة النَّاس من أجل سرقة أموالهم وبياناتهم.

2 يَدْرُسُ الْمُجْرِمُ الإلكترونيّ الصّحِيَّةَ لمعرفة نقاط ضعفها؛ لكسب الثّقة قبل القيام بجريمته.

3 الشّركات الكبرى لا تتعرّض أبداً لأيّ 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 مُجْرِمُو الاحتيال عبر الإنترنت إلّا إلى الحصول على الأموال فقط.



استخدام التطبيقات غير القانونية يُساعد مرتكبي جرائم الاحتيال عبر الإنترنت.

6

يمكن تحميل التطبيقات من أيّ موقع على الإنترنت دون خوف.

7

لا بأس من مشاركة البيانات والمعلومات السّريّة مع الآخرين عبر الهاتف.

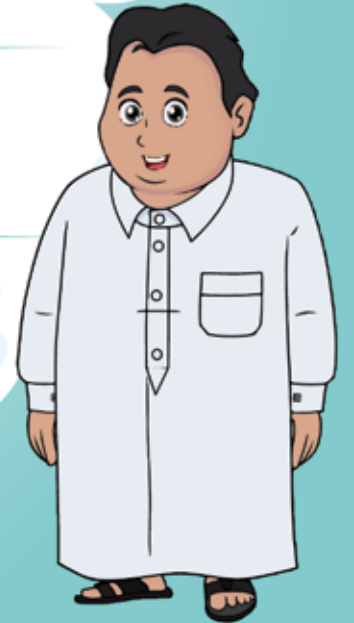
8

لا تحتاج إلى استخدام برامج مكافحة الفيروسات.

9

استخدم الأرقام من 1 إلى 8 كلمة مرور لحساباتك وأجهزتك.

10



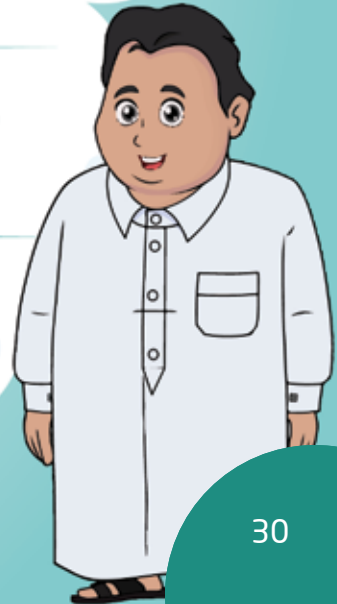
11 يمكنك التسوق من أي متجر إلكتروني ومشاركة بيانات بطاقتك البنكية دون خوف.

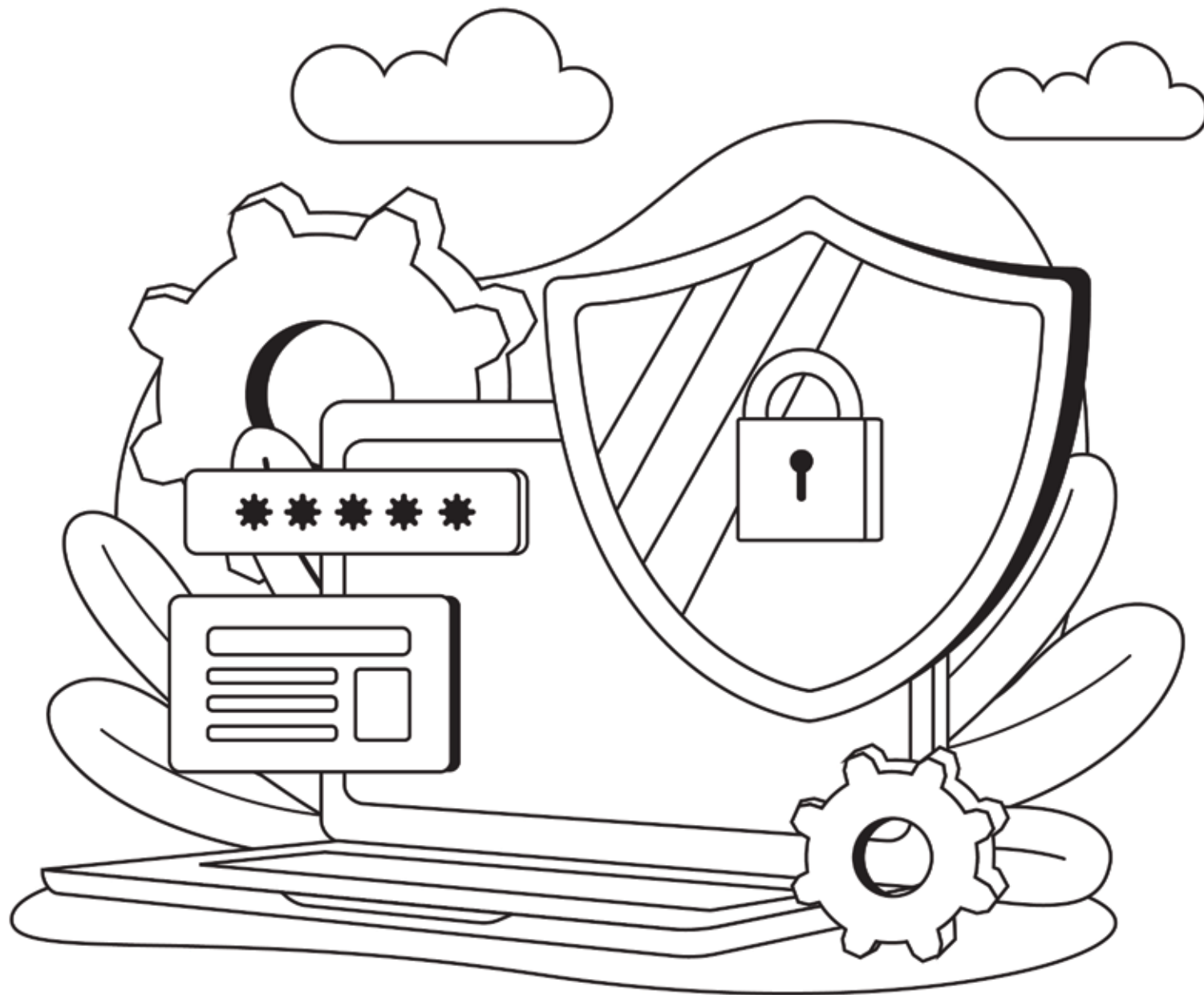
12 لا يمكن الاحتيال باسم المؤسسات الخيرية أو التطوعية.

13 التجارة الإلكترونية من أكثر الأهداف التي يستهدفها مجرمو الاحتيال عبر الإنترنت.

14 الروابط الخبيثة التي تُنقل عليها دون وعي قد تتسبب في سرقة بياناتك وحساباتك.

15 لا يمكن لفيروسات الفدية أن تتسبب في أي ضرر لأجهزتك أو بياناتك.





توجيه

اقرأ الجمل الواردة أدناه
بتمعن، وحدّد الكلمات
اللازمة لملء الفراغ ليصبح
للجملة معنى مفيد، وأدناه
مثال محلول.

التمرين الثالث

أكمل الجمل التالية:



1 **البصمة الرقمية** هي الظلّ الرقميّ، وتعني أثر البيانات التي تتركها عند استخدام الإنترنت.

2 تشمل البصمة الرقمية زيارات، ورسائل، والمعلومات التي تَبَحْث عنها.

3 البصمة الرقمية وهي حين تُشارك معلومات عن نفسك عن عَمْدٍ من خلال المشاركة في مواقع أو المنتديات.



البصمة الرقمية تحدث من خلال جَمْع المعلومات حول المُستخدِم دون أن يدرك ذلك، سواءً من زيارته للمواقع أو المعلومات التي يبحث عنها ويستخدم فيها عنوان الـ الخاص به.

4

للبصمة الرقمية أهمية كبيرة، خاصةً أنها تُقدِّم بيانات، وتُحدِّد سُمعة، وتلجأ بعض جهات العمل إلى تتبُّع الرقمية الخاصة بالموظفين المُحتَمَلين، ويمكن أن يُساء تفسير بعض الكلمات أو التي تُشاركها عبر الإنترنت، ممَّا يؤثر على سُمعتك أو الرقمية.

5

التمرين الرابع

كيف يمكنك حماية نفسك من
الاحتيال عبر الإنترنت؟
ضع علامة «✓» أو «✗»

توجيه

اقرأ الجمل الواردة بتمعن،
وفكر بدقة فيما إذا كانت
الجمل صحيحة أم خاطئة،
ويوجد مثال محلول.



1. تحميل تطبيقات موثوقة من المتاجر الرسمية.

2. استخدام نسخ معدلة ومسرّبة من التطبيقات الخاصة بالهواتف المحمولة.

3. استخدام برامج مكافحة الفيروسات وجدران الحماية.

4. مشاركة البيانات الشخصية عبر منصات التواصل الاجتماعي.

5. مشاركة البيانات عبر الاتصالات الهاتفية.

6. التسوق من المتاجر الموثوقة فقط.

7. تجنب مشاركة بيانات البطاقات البنكية عبر المواقع الإلكترونية.

8. لا بأس بالدخول إلى الروابط مجهولة المصدر.

9. اخذ الاستعانة بأطراف مجهولة في أثناء عمليات تحويل الأموال أو استلامها.

10. اختر كلمة مرور معقدة مكوّنة من حروف كبيرة وصغيرة وأرقام وبعض الرموز.

التمرين الخامس

حدّد الخطأ الذي وقع فيه
كلّ ضحية من ضحايا جرائم
الاحتيال عبر الإنترنت
التالية:

وَصَلَ إلى حمد بريد إلكترونيّ بهدية "iPhone 14"، فقام على الفور بفتح
الرّابط الموجود أمامه، ولكنّه لم يَصِل إلى شيء.

وَصَلَتْ رسالة من رقم دوليّ إلى هاتف "هالة" تطلّب منها إرسال كلمة
المرور الخاصّة بحسابها على Facebook، وفور إرسالها لم تتمكّن من
الدّخول إلى حسابها من جديد.



تواصل أحد موظفي خدمة العملاء في البنك مع "عبد الله" ليتأكد من صحة بيانات بطاقته وحسابه البنكي، وبعدها وجد عبد الله رسالة تخبره بسحب 50 ألف ريال من حسابه.

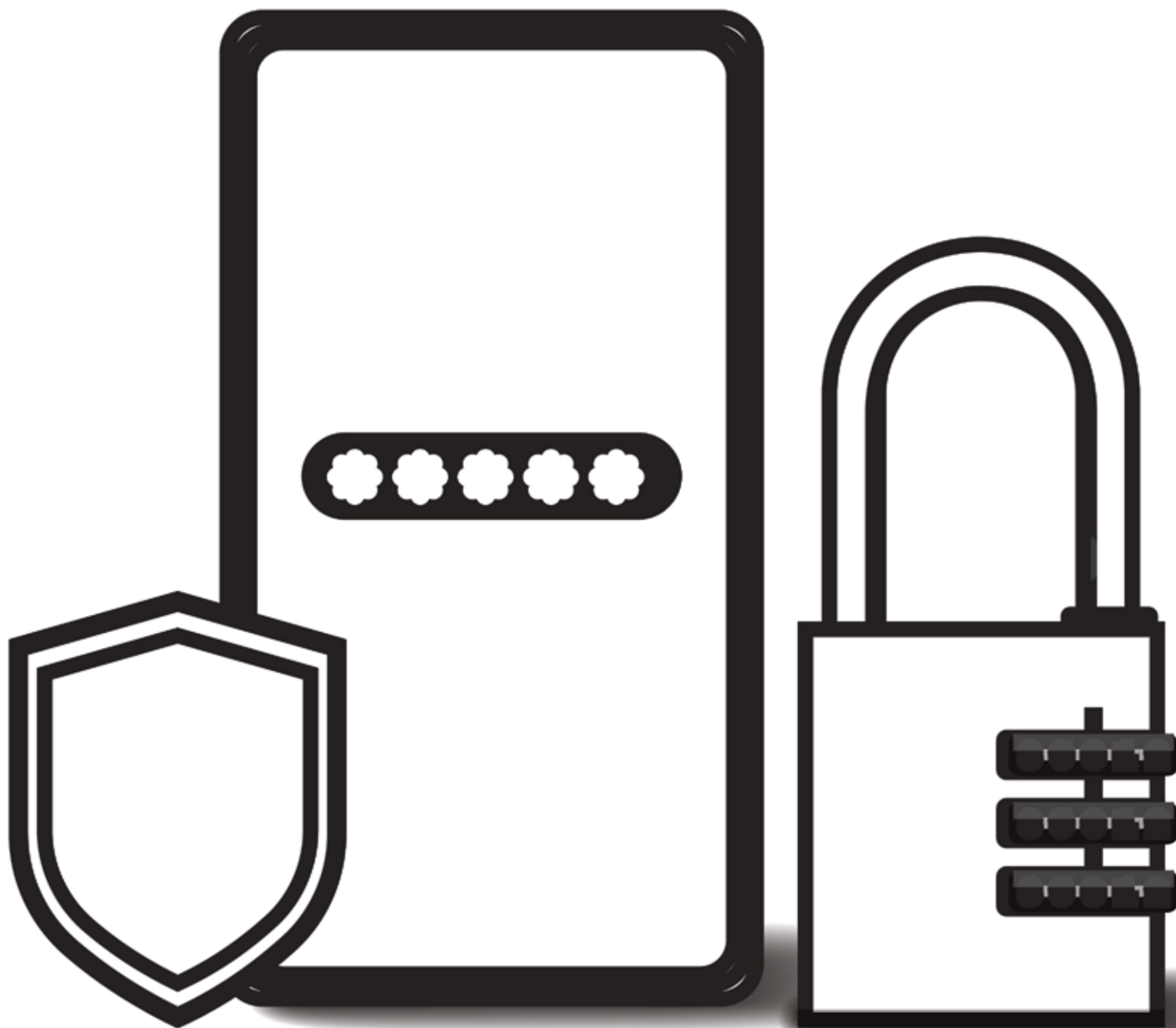
شاهدت "منى" إعلانًا ممولًا على Facebook لجمعية تجمع التبرعات للأجنيين في بعض الدول، فأرسلت إليهم مبلغًا من المال، وحين حاولت التواصل معهم للتأكد من وصول هذا المبلغ، لم تجد أي شخص يرد عليها.



هل تعلم؟

تسجيل الدخول إلى بعض مواقع الإنترنت باستخدام بيانات حسابك على Facebook قد يُعرضك للاحتيال عبر الإنترنت.





تَتَكَوَّنُ البَصْمَةُ الرَّقْمِيَّةُ مِنْ خِلَالِ

1 التَّسَوُّقُ عِبْرَ الْإِنْتَرْنَتِ.

2 التَّسْجِيلُ لِإِنْشَاءِ حَسَابٍ عَلَى مَوْقِعٍ وَبِئِيبٍ مَعْيِنٍ.

3 تَنْزِيلُ التَّطْبِيقَاتِ وَاسْتِخْدَامُهَا.

4 اسْتِخْدَامُ وَسَائِلِ التَّوَاصُلِ الْاجْتِمَاعِيِّ عَلَى الْأَجْهَازَةِ الْخَاصَّةِ بِكَ.

5 تَسْجِيلُ الدُّخُولِ إِلَى مَوَاقِعِ الْوَيْبِ الْآخَرَى بِاسْتِخْدَامِ بَيَانَاتِ Facebook.

6 التَّوَاصُلُ مَعَ الْأَصْدِقَاءِ وَجِهَاتِ الْإِتِّصَالِ عِبْرَ الْإِنْتَرْنَتِ.

7 مِشَارَكَةُ الْمَعْلُومَاتِ وَالبَيَانَاتِ وَالصُّوَرِ مَعَ مَعَارِفِكَ.

طرق حماية البصمة الرقمية

1 التَّحَقُّق من المعلومات الخاصّة بنا عبر استخدام محرّكات البحث.

2 إزالة المعلومات الشّخصيّة من المواقع الإلكترونيّة.

3 تقييد كمّيّة البيانات التي يتمّ مشاركتها على الإنترنت.

4 التَّحَقُّق من إعدادات الخصوصية بمواقع التّواصل الاجتماعيّ.

5 تجنّب المواقع غير الآمنة.

6 الحذر عند استخدام شبكة Wi-Fi عامّة.

7 حذف الحسابات القديمة الخاصّة بنا على الإنترنت.

8 إنشاء كلمات مرور قويّة.

9 عدم تسجيل الدّخول إلى مواقع الإنترنت باستخدام بيانات Facebook.

10 تحديث البرامج والتّطبيقات باستمرار.

11 تعيين كلمة مرور للهاتف المحمول.

12 التّحرّك بسرعة بعد انتهاك البيانات.

إرشادات الحماية من الاحتيال عبر الإنترنت

1 تحميل التطبيقات من المتاجر المعروفة.

2 تحديث نظام الهاتف.

3 تجنّب الروابط مجهولة المصدر.

4 الحذر من المعاملات التي تتضمّن أطرافًا مجهولة، مثل تحويلات الأموال.

5 الاستعانة ببرامج مكافحة الفيروسات.

6 استخدام كلمات مرور قويّة، وتغييرها بين الحين والآخر.

7 عدم التسوّق عبر المواقع المجهولة.





أمان المعلومات

مجموعة من الإجراءات والأدوات الأمنية التي تحمي على نطاق واسع المعلومات الحساسة من سوء الاستخدام أو الوصول غير المصرح به أو التعتيل أو الإتلاف.





اختر الإجابة الصحيحة

1. أي مما يلي يُعدّ من الأمثلة على البصمة الرقمية النشطة؟

المنشورات على منصات التواصل الاجتماعي. ☐

التطبيقات التي تستخدم تحديد الموقع الجغرافي. ☐

مواقع الويب التي تُنَبِّه ملفات الارتباط دون إخطار المستخدم. ☐

2. من أهم مصادر المعلومات الشخصية روابط التعريف الخاصة بالتطبيقات والمواقع الإلكترونية.

صحيح. ☐

خطأ. ☐

3. تتم عملية الاحتيال عبر الإنترنت عادةً عند زيارة الأفراد للمواقع الإلكترونية أو غرف الدردشة أو المتاجر

الإلكترونية أو المدونات أو التطبيقات.

صحيح. ☐

خطأ. ☐





4. الخداع أو الفِش المعلوماتي من المفاهيم المرتبطة بمفهوم الاحتيال عبر الإنترنت، ويُطلق عليه "الاحتيال المعلوماتي".

صحيح. ☐

خطأ. ☐

5. النّصب عبر الإنترنت هو الاستيلاء على مال الآخرين بواسطة الخداع، من خلال استخدام أجهزة الحاسوب والهواتف الذكية والأجهزة اللوحية.

صحيح. ☐

خطأ. ☐

6. من أسباب الاحتيال عبر الإنترنت:

عدم اتباع قواعد التصفح الآمن للإنترنت. ☐

التعامل مع المتاجر الإلكترونية غير الموثوقة. ☐

استغلال مشاعر التعاطف. ☐

جميع ما سبق. ☐





7. رسائل البريد الإلكتروني التي تتضمّن روابط مسابقات أو جوائز مالية وعينية مغرية من أشكال الاحتيال عبر الإنترنت.

صحيح. ☐

خطأ. ☐

8. الثغرة الأمنية هو مصطلح يُطلق على مناطق القوة في أنظمة تشغيل الحاسوب والبرامج.

صحيح. ☐

خطأ. ☐



9. لا تُمثّل الثغرات غير المكتشفة Zero-Day تهديدًا للأمن السيبراني.

صحيح. ☐

خطأ. ☐



10. خطوة "إنشاء رمز الاستغلال" تقع ضمن آلية عمل هجوم الثغرات غير المكتشفة Zero-Day.

صحيح. ☐

خطأ. ☐

11. كلمة "سرقة" في عالم الإنترنت يُطلق عليها

انتهاك البيانات. ☐

تسريب البيانات. ☐

جميع ما سبق. ☐

12. يمكن استخدام لتتبع أنشطة أي شخص عبر الإنترنت.

بصمة الوجه. ☐

بصمة اليد. ☐

البصمة الرقمية. ☐



اعثر على العنصر المطابق

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

العمود (أ)

- ☐ من أدوات الاحتيال عبر الإنترنت
- ☐ رسائل البريد الإلكتروني المزيفة
- ☐ من أمثلة جرائم الاحتيال عبر الإنترنت
- ☐ إحدى الثغرات الأمنية التي تُصيب البرمجيات
- ☐ مجموعة من الإجراءات والأدوات الأمنية التي تحمي المعلومات الحساسة من سوء الاستخدام
- ☐ سرقة معلومات رقمية مخزنة على أجهزة الحاسوب أو الهواتف بغرض انتهاك الخصوصية
- ☐ مرادف كلمة سرقة في مجال الإنترنت

العمود (ب)

- ☒ سرقة البيانات.
- ☒ الاحتيال عبر الإنترنت.
- ☒ أمان المعلومات.
- ☒ سرقة العملات الرقمية، مثل البيتكوين.
- ☒ استغلال حالات الطوارئ، مثل جائحة كورونا.
- ☒ أحد أشكال الاحتيال عبر الإنترنت.
- ☒ الثغرات غير المكتشفة Zero-Day.

ضع الكلمة أو العبرة المرادفة للجمل التالية

هجوم تتعرض له يُعطّل حساباتنا على الإنترنت، ومقابل إعادة استخدامها علينا دفع مبلغ ماليّ.

رسائل بجوائز ماليّة وهدايا مُزيّفة تصل إلينا عبر البريد الإلكترونيّ أو Messenger، وهَدَفُها خِداعنا وسرقة بياناتنا.

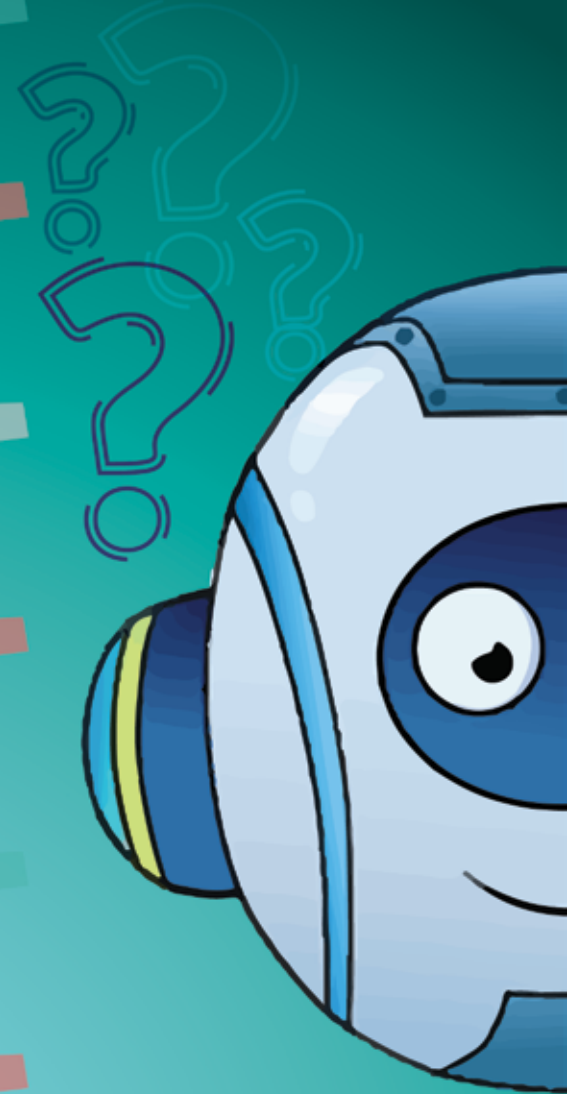
نقاط ضعف تتسبّب في اختراق أجهزتنا، سواء الحاسوب أو الهاتف الذكيّ أو الأجهزة اللّوحية، وتُعرّضنا للخطر.

أدوات تحمي معلوماتنا الحسّاسة من الوصول إليها وتعطيها أو إتلافها.

سرقة من نوع خاصّ تستهدف بياناتنا الشّخصيّة على الإنترنت ويعاقب القانون فاعلها.

آثار على الإنترنت يستخدمها المهاجمون لاستغلال ما بها من معلومات وبيانات حسّاسة لخداعنا وكذلك خداع الآخرين.

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





أكمل الجمل التالية بالإجابات الصحيحة:

1 البصمات الرقمية يُقصد بها مشاركة المُستخدم معلومات عن نفسه عمدًا.

2 البصمة الرقمية يُقصد بها جَمْع معلومات حول المُستخدم دون أن يدرك أن هذا يحدث.

3 يستطيع مُجرمو الإنترنت استغلال لأغراض مثل سرقة الهوية عبر الإنترنت.

4 من بين الطرق التي يُضيف بها المستخدمون إلى بصمتهم الرقمية تنزيل

5 من طرق حماية البصمة الرقمية تقييد



6 التَّحَقَّق من إعدادات الخصوصية من طرق حماية

7 من إرشادات الحماية من الاحتيال عبر الإنترنت تجنّب الروابط

8 يَفْضَل أن تُسْتَخْدَم كلمات مرور مَكُونَة من للحماية من الاحتيال عبر الإنترنت.

9 في حال التَّعَرُّض لجريمة الاحتيال عبر الإنترنت نلجأ إلى إبلاغ

10 إذا كانت شاشتك تمتلئ بِشَكْلِ مفاجئٍ بالتَّوافذ المنبثقة، فيجب

انتبه!

البصمة الرقمية

تُشير إلى أثر البيانات والمعلومات التي تتركها عند استخدام الإنترنت، وهي تشمل مواقع الويب التي تزورها، ورسائل البريد الإلكتروني التي ترسلها وتستقبلها، والمعلومات التي تُقدمها عبر الإنترنت.

وتُحدد **البصمة الرقمية** سُمعة الأشخاص على الإنترنت كما يحدث في الحياة العادية.





مشروع التَّخْرِج هو واجب يقوم به الطَّالِب بمفرده أو بالاشتراك مع زميل أو أكثر، ويقوم من خلاله وتحت إشراف المُدَرِّب بأحد الواجبات التالية:

مشروع التَّخْرِج



يَتَقَمَّص الطَّالِب دَوْر المُدَرِّب وَيَكْتُب تَوْجِيهَاتٍ عَامَّةً لَزَمَلَانِهِ أَوْ أَهْلِهِ يَوْضَحُ لَهُمْ فِيهَا الإِجْرَاءَاتِ الْمَطْلُوبَةَ لِلوَقَايَةِ مِنْ مَخَاطِر التَّزْوِيرِ وَالْإِحْتِيَالِ عِبْرَ الْإِنْتَرْنِتِ.



كُتَابَةُ قِصَّةٍ قَصِيرَةٍ تَحْدُورُ أَحْدَاثُهَا حَوْلَ طَالِبٍ تَعْرِضُ لِمَحَاوَلَةِ إِحْتِيَالٍ عِبْرَ الْإِنْتَرْنِتِ، وَكَيْفَ تَصَرَّفَ جِيَالُ هَذَا الْمَوْقِفِ.







CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency