

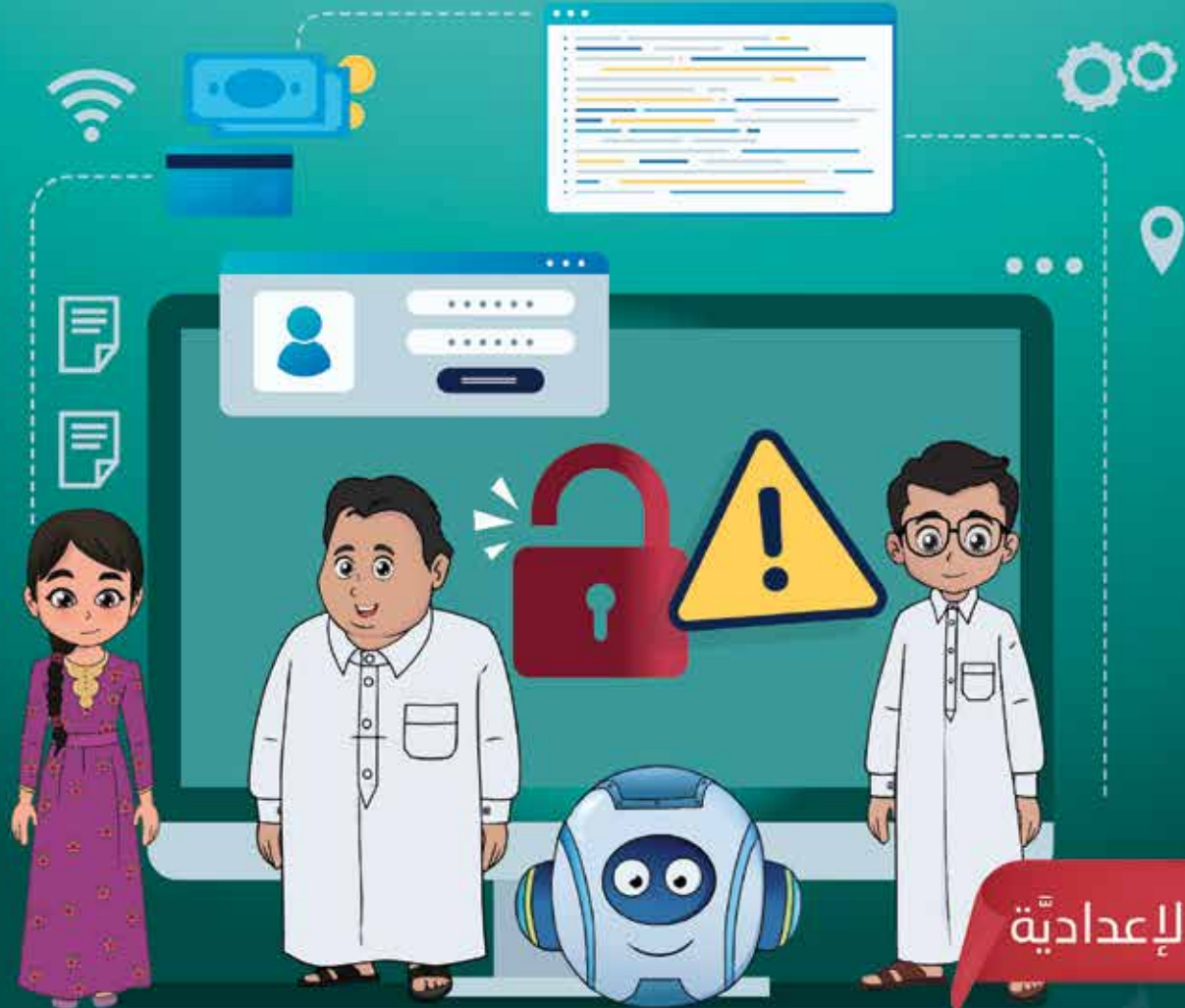
التزوير والاحتيال عبر الإنترنت

خاصة بالمدرّب

الحقيّة التدريبيّة



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



المرحلة الإعداديّة

التزوير والاحتيال عبر الإنترنت

المرحلة الإعدادية

المادة التدريبية

(حقيية خاصة بالمُدرب)

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/>

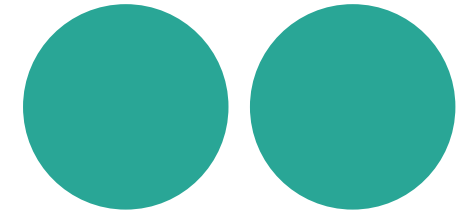
✉ cyberexcellence@ncsa.gov.qa

☎ 00974 404 663 78

☎ 00974 404 663 62

المحتوى العام للحقيبة

أولاً: مدخل عام للحقيبة
ثانياً: المادة العلمية



أولاً: مَدْخُل عامٌّ إلى الحَقِيقَةِ التَّدْرِيبِيَّةِ

فيما يلي تبيان لبعض التفاصيل ذات الصلة المباشرة بأهداف الحَقِيقَةِ التَّدْرِيبِيَّةِ، مع توجيهات عامة للمُدَرِّب حول كيفية التَّعامل مع هذه الحَقِيقَةِ وتزويده بالمحتوى العِلْمِيّ الذي سَيَقْتَمِد عليه في التَّدْرِيب.

الفكرة العامة

أهداف الحَقِيقَةِ التَّدْرِيبِيَّةِ

- تقوم فكرة هذه الحَقِيقَةِ التَّدْرِيبِيَّةِ على تزويد المُدَرِّب بأدوات ووسائل تدريبيّة؛ بحيث يسهل عليه تقديم المعلومات للمتدربين. وبشكل عام فإنّ كلّ مادّة تدريبيّة تكون على جزأين؛ جزء لدى المُتَدَرِّب وجزء آخر لدى المُدَرِّب، والحَقِيقَةِ التَّدْرِيبِيَّةِ تُعدّ بمثابة مُوجّه عامٍّ للمُدَرِّب وداعِم له، ومحتواها العِلْمِيّ هو ذاته لدى المُتَدَرِّب، ولكنّ بأسلوب عَرَض مُخْتَلَف؛ إضافةً إلى تزويد المُدَرِّب بأدوات ووسائل تدريب تدعّمه في عملية التَّدْرِيب.
- تزويد المُدَرِّب بوسائل تدريب تُساعده على إيصال المحتوى التدريبيّ للطلبة.
- تقديم المعلومات والمحتوى التدريبيّ بشكلٍ سهّل ومُبَسَّط.
- تقديم المحتوى التدريبيّ الخاصّ بالتزوير والاحتيال عبر الإنترنت . مُرفقًا بأدوات ووسائل تدريب مُتَعَدِّدَة .

محتوى الحقيبة التدريبية

تتضمن الحقيبة التدريبية عدّة أدوات تدريبية، فيما يلي تبيان لها:

1. ملفّ العرض.
2. ألعاب تدريبية، كالکلمات المتقاطعة ملء الفراغات، يقوم المدرب بعرضها على الطلبة؛ بهدف ضمان تفاعلهم مع المحتوى التدريبي.
3. فيديوهات تعليمية.
4. مسابقات، وهي على شكل أسئلة استنتاجية يعرضها المدرب على الطلبة بهدف التفاعل فيما بينهم.
5. بطاقات تدريبية، وهي على شكل معلومات عامة مرفقة بصور تعبيرية، يعرضها المدرب على الطلبة.
6. إكتشات، تتضمن معلومات حول المحاور الرئيسة في المحتوى التدريبي.

فَهْرَسُ الْمُحْتَوَى الْعِلْمِيِّ

الفصل الأول

مفهوم التزوير والاحتيال عبر الإنترنت وأنواعه.....19

- أولًا: مفهوم الاحتيال عبر الإنترنت.....21
- ثانيًا: أسباب الوقوع ضحية للاحتيال عبر الإنترنت.....23
- ثالثًا: أنواع وأشكال الاحتيال عبر الإنترنت.....24

الفصل الثاني

كيفية تنفيذ عمليات الاحتيال عبر الإنترنت.....27

- أولًا: الثغرات المُساعدة على عمليات الاحتيال عبر الإنترنت... 29
- ثانيًا: أمن البيانات الشخصية والاحتيال عبر الإنترنت.....32
- ثالثًا: البصمة الرقمية والاحتيال عبر الإنترنت.....33

الفصل الثالث

كيفية التصرف في حال التعرض للاحتيال عبر الإنترنت.....41

- أولًا: إرشادات الحماية من الاحتيال عبر الإنترنت.....43
- ثانيًا: حماية البيانات من الاحتيال عبر الإنترنت.....44
- ثالثًا: الجهات التي أُلجأ إليها عند تعرضي للاحتيال

عبر الإنترنت.....46

تمارين وتدرّيات.....49

مراجع المحتوى العلمي في الحقيقة

التوزيع الزمني للورشة

المحتوى	الوقت المخصص
تمهيد	5 دقائق
الجزء النظري من المادة	25 دقيقة
عرض الفيديوهات التعليمية	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الألعاب التدريبية	25 دقيقة
حوار ونقاش مع الطلبة	15 دقيقة
مشروع التخرج	5 دقائق
المدة الزمنية للورشة	ساعتان

دليل إرشادي للمُدرِّب

فيما يلي تبيان لبعض الإرشادات العامة للمُدرِّب، والتي تتمحور حول كيفية استخدام هذه الحَقِيبة.

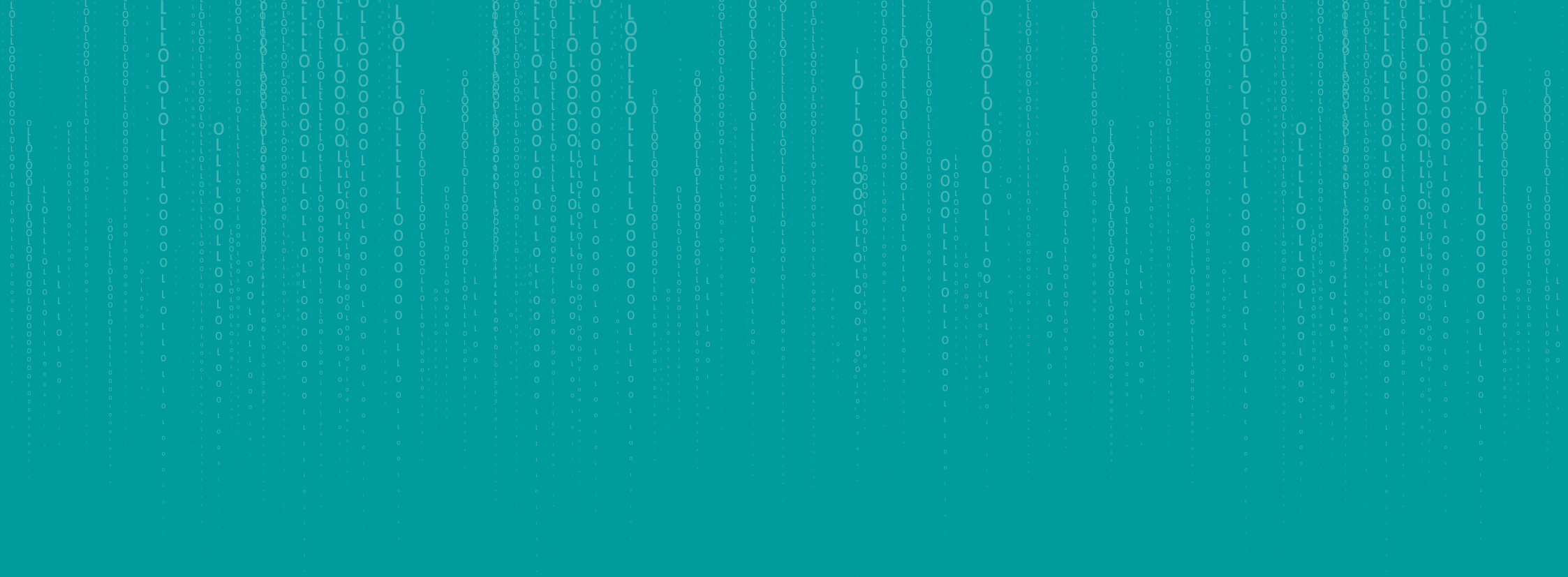
1. المحتوى العلمي للحَقِيبة قد يكون يَفوق قُدرة الطَّلِبة على الاستيعاب؛ خاصَّة من ناحية المصطلحات والمفاهيم العامة؛ لذلك لا بُدَّ للمُدرِّب أن يقوم بتبسيط هذه المفاهيم وتقديمها بصورة قابلة للفهم من قِبَل طَلِبة المَرحلة الإِعدادِيَّة.
2. يقوم المُدرِّب بعرض شرائح العرض عند كُل نقطة يتحدَّث عنها، فمثلاً عند الحديث عن مفهومي التَّزوير والاحتِيال عبر الإنترنت . يقوم بعرض الشَّرائح التي تتناول ذات الفِكرة
3. عَقِب شَرْح القُصَلين الأوَّل والثَّاني من المادَّة العِلْمِيَّة يتمَّ إعطاء اختبار بسيط لهم هو "ضع علامة (✓) أو علامة (X) أمام كُل جُملة".
4. في أثناء شرح القُصَل الأوَّل يتمَّ توزيع الصُّور المصمَّمة خِصيصاً لفِقرة "هل تعلم أن...؟".
5. يعرض المُدرِّب الجزء الخاص بـ "إسكتشات" أثناء قيام الطَّلِبة بحل التَّمارين والتَّدريبات.
6. في نهاية التَّدريب يتمَّ عرض أسئلة المُسابقات المذكورة في نهاية الملف.
7. في أثناء عرض المادَّة العِلْمِيَّة لِكُل قُصَل يتمَّ استقطاع فترة من الوقت المُخصَّص له لعرض عددٍ من الرِّوابط ذات الصِّلة بمضمون القُصَل.
8. يقوم المُدرِّب بعرض الفيديوهات -المذكورة في ملفِّ مُنفصل- على الطَّلِبة في نهاية كُل قُصَل، أو في المَوْضِع الذي يراه مُناسِباً.
9. ذُكر أمثلة عن حَوادِث تَزويرٍ واحتِيالٍ إلكترونيٍّ حدثت خلال عرض المادَّة العِلْمِيَّة.
10. يُرجى فتح باب المُناقشة مع الطَّلِبة في المَوَاضِع التي يراها المُدرِّب مُناسِبة.
11. فيما يخصُّ التَّمارين المَوْجَّهة للطَّلِبة؛ سيتمَّ إرفاق ملفِّ التَّمارين في نهاية هذه الحَقِيبة، وهذه التَّمارين تُقسَّم لجزأين؛ جُزء يتمَّ تقديمه للطَّلِبة خلال التَّدريب، وهو تمارين صَفِيَّة، والجُزء الآخر يُكلِّف الطَّلِبة بالإجابة عنه في المنزل، وهو تمارين لاصِفِيَّة، وسيتمَّ توضيح هذه الجُزئية في نهاية هذه الحَقِيبة.



مشروع التخرج

مشروع التخرج هو عمل يقوم به الطالب، ويهدف لتحقيق عدة أهداف، فيما يلي تبيان لأهمها:

- التأكد من أن الطالب قد استوعب المعلومات والأفكار التي تم تقديمها له، وأنه بات قادراً على الاستفادة منها في حياته اليومية.
- ترسيخ المعلومات والأفكار التي تم تقديمها للطالب.
- المشروع بمثابة رَبط بين الأفكار والمعلومات النظرية بالواقع العملي والتطبيقي.
- كتابة قصة قصيرة تدور أحداثها حول طالب تعرض لمحاولة اختيالي عبر الإنترنت، وكيف تصرف حيال هذا الموقف.
- يتقمص الطالب دور المُدرِّب ويكتب توجيهات عامة لزملائه أو أهله يوضح لهم الإجراءات المطلوبة للوقاية من مخاطر التزوير والاحتيال عبر الإنترنت.
- وفيما يتعلق بآلية تكليف الطلبة بالمشروع وكيفية تنفيذه، يمكن تقديم التوجيهات التالية:
- يمكن أن يكون مشروع التخرج فردياً أو جماعياً، وفي حال كان جماعياً يجب ألا يتجاوز عدد الطلبة المشتركين في مشروع واحد ثلاثة طلبة.
- اختيار موضوع المشروع يكون من قبل الطلبة، ويمكن للمدرِّب تقديم بعض المساعدة أو الأفكار في هذا المجال.



ثانيًا: المادّة العِلْمِيّة

مقدمة

ووفقًا لتقرير حالة مُرونة الأمن السيبراني لعام 2021م من Accenture، زادت الهجمات الرقمية بنسبة 31% بين عامي 2020م - 2022م، وزاد عدد الهجمات لكل شركة من 206 إلى 270 على أساس سنوي، وبالطبع تلك الهجمات تؤثر على الأفراد أيضًا لأن العديد من الشركات تحتفظ ببيانات مهمة ومعلومات شخصية خاصة بالعملاء. فيمكن لهجوم واحد، سواء كان خرقًا للبيانات أو برمجيات خبيثة أو برنامج طَلَب فدية أو هُجوم حرمان من الخدمات، أن يكلف الشركات من جميع الأحجام ما متوسطه 200 ألف دولار⁽¹⁾.

وفي عام 2021م نشرت Javelin Strategy & Research دراسةً عن اختيال الهوية أوضحت فيها أن خسائر هذا النوع من الجرائم الإلكترونية بلغت (56 مليار دولار)⁽²⁾؛ أما بالنسبة للأفراد فقد يكون تأثير الجريمة الإلكترونية عميقًا، مُخلفًا ضررًا ماليًا في المقام الأول، وأيضًا فقدان الثقة والإضرار بالسمعة.

في ظل الطفرة الرقمية التي يشهدها عالمنا اليوم، تداول على مَرَأى ومَسْمَع منا جميعًا الكثير من المصطلحات المُستحدثة ذات الصلة بعالم الجريمة، كما هو الحال مع الجرائم الإلكترونية التي تستهدف أجهزة الحاسوب والشبكات، وتحاول استغلالهم في القيام بأنشطة إجرامية لكسب المال أو التسبب في ضرر لمالكيها لأسباب شخصية، وتقع معظم الجرائم الإلكترونية على أيدي القراصنة أو الهاكرز.

وتتعدّد أنواع وأشكال الجريمة الإلكترونية، فهناك الاختيال عبر البريد الإلكتروني والإنترنت وتزوير الهوية، حيث تتم سرقة المعلومات الشخصية واستخدامها، وكذلك سرقة البيانات المالية أو بيانات الدفَع بالبطاقة، وأيضًا الابتزاز الإلكتروني الذي يتم فيه تهديد بعض الشخصيات مقابل الحصول على مالٍ، ويُطلق على هذا النوع من الجرائم أيضًا (هجمات برمجيات الفدية). إضافةً إلى جرائم انتهاك حقوق النشر والتأليف، وبيع السلع غير المشروعة عبر الإنترنت.

1. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: <https://cutt.us/ZMXpw>

2. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: <https://cutt.us/fVN5g>

الفصل الأول

مفهوم التزوير والاحتيال عبر الإنترنت وأنواعه

- أولاً: مفهوم الاحتيال عبر الإنترنت
- ثانياً: أسباب الوقوع ضحيةً للاحتيال عبر الإنترنت
- ثالثاً: أنواع وأشكال الاحتيال عبر الإنترنت



أولاً: مفهوم الاحتيال عبر الإنترنت

على العملاء والمستخدمين عن طريق سرقة الأموال والمعلومات الشخصية المهمة وغيرها من البيانات؛ وعادةً تكون هجمات الاحتيال عبر الإنترنت بهدف التجسس أو انتحال الشخصية أو الحصول على معلومات حساب المستخدمين في مراكز مهمة أو على صلة بأشخاص مهمين (أي لأسباب شخصية)، وقد تكون لسرقة الأموال من الحسابات المصرفية وبطاقات الدفع الإلكترونية⁽¹⁾.

وتتم عملية الاختراق (الاحتيال عبر الإنترنت) عادةً عند زيارة الأفراد للمواقع الإلكترونية أو غرف الدردشة (الماسنجر) أو المتاجر الإلكترونية أو المدونات أو التطبيقات الذكية، وفي هذه المرحلة يتم الإيقاع بالضحية عبر نصب أحد الفخاخ الإلكترونية له، ليقوم المجرم بتنفيذ بقية خطته غير المشروعة عن طريق الهجوم على بيانات الأشخاص وحسابات العملاء.

الاحتيال عبر الإنترنت هو أحد أشهر أنواع الجرائم الإلكترونية انتشارًا، ومما ساعد على انتشاره في السنوات الأخيرة تزايد عدد مستخدمي الإنترنت وتطبيقاته المختلفة، كوسائل الدفع الإلكتروني وانتشار وسائل التواصل الاجتماعي وغيرها، إذ زادت جرائم التصيد والاحتيال على الأفراد بالتزامن مع ارتفاع أعداد الأشخاص على شبكة الإنترنت وتداخلها في جميع جوانب الحياة الاقتصادية والتجارية والسياسية والاجتماعية، فأصبح العمل والتسوق والترفيه أمرًا يمكن إجراؤه على شبكة الإنترنت بسهولة وسرعة من خلال هاتف ذكيّ مربوط بشبكة إنترنت.

يعدّ الاحتيال عبر الإنترنت من أسهل الجرائم الإلكترونية ارتكابًا كونها لا تحتاج إلى خبراء أو برامج متخصصة أو متخصصين في مجال الهاكرز والقرصنة، بل يمكن تنفيذ هذه الجريمة عن طريق حسابات مواقع التواصل الاجتماعي عبر انتحال الشخصية والاحتيال عبر غرف الدردشة؛ ويشار إلى الاحتيال عبر الإنترنت على أنه 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

1. Internet Fraud, Australian Federal Police (AFP). on site: <https://cutt.us/leAYp>

تعريف جريمة الاحتيال عبر الإنترنت

الآخرين بوسيلة يشوبها الخداع؛ مما يتسبب في سرقة هذا المال عن طريق أجهزة الحاسوب.

وهنا يقوم الجاني "المهاجمون الإلكترونيون" باستخدام تقنيات حديثة بغرض التلاعب في البيانات المصرفية والمستحقات المالية، وكذلك الميزانيات للشركات لتحويل المال في أسرع وقت لحسابه الشخصي، بالطبع هذا النوع من الهجمات الإلكترونية يؤثر سلباً على الاقتصاد الوطني؛ فقد يؤدي إلى إفلاس البنوك والشركات.



تُعرف جريمة الاحتيال عبر الإنترنت بأنها التلاعب القمد بمعلومات وبيانات تمثل قيمة مادية يختزنها نظام الحاسوب أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة أو التلاعب في الأوامر والتعليمات من خلال عملية البرمجة أو أية وسيلة أخرى، من شأنها التأثير على الحاسوب حتى يقوم بعملياته بناءً على هذه الأوامر أو البيانات أو التعليمات من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالآخرين. ويمكن إدارة العملية الإجرامية من مكان بعيد عن مسرح الجريمة ذاتها، أو من خارج حدود الدولة مثل جرائم الاحتيال الخاصة بترويج المواد غير الملائمة وكذلك النصب الإلكتروني⁽¹⁾.

وترتبط بالاحتيال عبر الإنترنت مجموعة من المفاهيم الأخرى، مثل مفهوم الاحتيال المعلوماتي، والذي يقصد به: الخداع أو الغش المعلوماتي الذي يقوم على التلاعب في نظم المعالجة الآلية للمعلومات بغرض الحصول دون وجه حق على خدمات أو أموال أو أصول معينة؛ وكذلك مفهوم "الاحتيال أو النصب المالي الإلكتروني" ويقصد به: الاستيلاء على مال

1. يونس الباشا، فايزة، الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية، دار النهضة العربية للطبع والنشر والتوزيع، 2001م، ص 21.

ثانيًا: أسباب الوُقوع ضحيةً للاختيال عبر الإنترنت

- تتعدّد الأسباب المؤدّية إلى جرائم الاختيال عبر الإنترنت، وغالبًا ما تكون بسبب الاستخدام الخاطئ لوسائل التواصل الاجتماعيّ وشبكة الإنترنت، وعدم اتّباع قواعد التعامل الآمن مع الإنترنت، وعدم الوعي الثّامّ بمفاهيم الأمن السيبرانيّ والسّلامة الرّقمية.
 - وفيما يلي تبيان لأهمّ العوامل والأسباب التي تُؤدّي إلى وُقوع مُستخدمي الإنترنت ضحيةً للاختيال عبر الإنترنت:
 - قلة الوعي بأهميّة قواعد الاستخدام الآمن للإنترنت.
 - التسرّع في اتّخاذ القرار عند تصفّح المواقع الإلكترونيّة، أو عند فتح رسائل البريد الإلكترونيّ، فقد يتسرّع المُستخدم في التعامل مع أيّ رابط يحدّه أمامه، وهو أسلوبٌ يتّبعه المُحتالون على الإنترنت لعدم إعطاء المُستهذفين الفرصة للتّفكير أو التّحقّق من مصداقيّة الرّسالة التي تلقّوها.
 - الدّخول إلى مواقع إنترنت غير آمنة، وعندها يتلقّى المُستخدم إشعارات أو رسائل وهميّة، غالبًا تُشير إلى أنّ المُستخدم قد ربّح أموالًا أو أجهزةً إلكترونيّةً، وتطلّب منه تزويدها ببيانات ومعلومات شخصيّة لِشُسلّمه الهدية، وفور إدخال المُستخدم لأيّ بياناتٍ شخصيّة سيكون قد وقع ضحيةً للاختيال.
- نُشر معلوماتٍ شخصيّةٍ على مواقع التواصل الاجتماعيّ، وهذه المعلومات تُشكّل فُرصة للمُحتالين للإيقاع بالمُستخدمين، ومن خلالها وبالاعتماد على البصمة الرّقمية للمُستخدم يُمكن الإيقاع به والاختيال عليه.
- التّعامل مع متاجر إلكترونيّة غير موثوقة، تُسقى لخداع المُستخدمين وسرقة أموالٍ من بطاقات الدّفع الإلكترونيّة الخاصّة بهم.
- انتشار منصات تبادل العُملة الرّقمية، مثل البيتكوين وغيرها، فحاليًا هناك العديد من المنصات لتبادل هذا النوع من العُملة، وبعضها يكون منصات وهميّة، تحتال على المُستخدمين، وقد تمّنحهم أحيانًا بعض الأموال بهدف كسب ثقتهم، ولاحقًا يتمّ خداعهم وسرقة أموالهم.
- انّحال المُحتالين لشخصيّات رسميّة أو شخصيّات عامّة، وهو ما يجذب أحيانًا بعض المُستخدمين للإنترنت، ولاحقًا يتمّ خداعهم.
- استغلال التعاطف الإنسانيّ، قد يقوم بعض المُحتالين بانتحال صفة منظمات أو أفراد يقومون بجمع تبرّعات لحالات إنسانيّة حادّة، وبعض هذه الحالات تكون غايتها الاختيال، لذلك لا يجوز دَفْع أيّ تبرّعات أو مُساعدات إلّا لمنظماتٍ معروفة وذات مواقع رسميّة وبموجب إيصالٍ مُصدّقة أصولًا.

ثالثاً: أنواع وأشكال الاحتيال عبر الإنترنت

لا توجد أنواع ثابتة أو دائمة للاحتيال عبر الإنترنت، فغالباً ما يسعى المُحتالون لتطوير أساليبهم، ولكنها بشكل عام تتم عبر أدوات ووسائل رئيسية.

وفيما يلي تبيان لأهم هذه الأدوات والأنواع:

البريد الإلكتروني:

قد يصل إلى البريد الإلكتروني رسائل تتضمن روابط مُسابقات أو جوائز مالية وعينية مُغرية مثل: الهواتف الذكية أو الحصول على فرصة قضاء العطلة في إحدى الدول الخارجية، وبمجرد الضغط على الرابط يُطلب من مالك البريد إدخال بعض البيانات الشخصية أو المالية مثل رقم بطاقته الائتمانية أو رقمه الوطني أو رقم جواز السفر... وغيرها من بيانات شخصية مهمة. وقد يُطلب منه أيضاً حوالة مالية ولو صغيرة من أجل الحصول على الجائزة. هذا الأمر يُعرض المعلومات الشخصية للخطر، ويزيد من فرص سرقة المال من الحسابات الخاصة.

ومن طرق الاحتيال عبر الإنترنت التي تُعد أكثر خداعاً ومكرًا، إرسال بريد إلكتروني مُزوّر يبدو كأنه أُرسِل من صديق أو جهة رسمية في حين أنها ليست سوى عملية تصيد إلكتروني؛ إذ يُطلب من الشخص معلومات مُعيّنة وحساسة. على سبيل المثال: قد تُخبرك الرسالة أنك في حاجة لتغيير كلمة المرور على حساب "PayPal" لأن هناك محاولة لاختراقه، وتبدو الرسالة كأنها من الموقع الرسمي، ما يزيد من احتمالية تنفيذ المطلوب وإدخال كلمة مُزوّر جديدة، وهو ما يسمح باستخدامها من طرف جهة الاحتيال لسرقة المال⁽¹⁾.

الهاتف الذكي والأجهزة اللوحية:

يتسبب تثبيت تطبيقات غير آمنة وكذلك الضغط على روابط مجهولة (غير معلوم مصدرها الأصلي أو مشكوك فيها) إلى اختراق البيانات الشخصية كالصور والملفات، وأيضاً سرقة بعض المعلومات مثل: كلمات المرور وأرقام البطاقات البنكية، ما يؤدي إلى وقوع الشخص ضحية في يد المجرمين

1. What is email fraud? Cloudflare. On site: <https://cutt.us/mg8Sf>

التجارة الإلكترونية:

مع نمو حجم ومكانة التجارة الإلكترونية ظهر شكل جديد من الاحتيال عبر الإنترنت يستهدف الضحايا من المتعاملين على المواقع الإلكترونية للمحال التجارية، أي يمكن أن يزور المستخدم موقعًا مزيفًا بهدف شراء بعض السلع إلا أنه يفاجأ بوقوعه ضحية للاحتيال والنصب الإلكتروني⁽³⁾، وهو ما يعني أنه سيدفع المال دون الحصول على أي مقابل. كما يمكن أن تحول بعض المواقع المزيفة المستخدم إلى طرق دفع إلكتروني غير معروفة، وذلك بهدف سرقة المعلومات البنكية.

استغلال الكوارث:

في وقت الأزمات مثل الكوارث الطبيعية أو الصحية مثل "جائحة كورونا" التي وقعت قبل سنوات، يلجأ مرتكبو الجرائم الإلكترونية إلى تنظيم حملات وهمية تدعو إلى التبرع من أجل مساعدة الضحايا، ما يتسبب في إعطائهم معلومات خاصة بالحسابات البنكية، وهو ما يقع تحت طائلة الاحتيال عبر الإنترنت.

الإلكترونيين وتعرضه للابتزاز مقابل دفع المال أو قد تستخدم بياناته الخاصة لمصلحة هؤلاء المجرمين؛ كما يمكن أن يتم الاحتيال عبر الإنترنت عبر انتحال صفة صديق على الإنترنت بتفيس الاسم والصورة الشخصية، بهدف طلب خدمة ما، مثل تحويل المال إلى رقم الهاتف أو استخدام معلومات شخصية⁽¹⁾.

الحاسوب:

تتضمن بعض أجهزة الحاسوب المملوكة للشركات والمؤسسات الكبيرة والصغيرة على حد سواء معلومات في غاية الأهمية، لذا يلجأ القرصنة والمحتالون إلى اختراق الحاسوب بالبرمجيات والروابط الخبيثة، مما يؤدي إلى توقفها عن العمل، بعدها يتم التواصل مع أصحاب تلك الشركات والمؤسسات بفرض ابتزازهم من أجل دفع المال مقابل استرجاع إمكانية الدخول إلى الحسابات الخاصة بهم للوصول إلى المعلومات المخزنة عليها⁽²⁾.

1. Mobile phone fraud, Action Fraud - National Fraud&Cyber Crime Reporting Centre. On site: <https://cutt.us/1FoJG>
2. Computer and Internet Fraud, Impact Law. On site: <https://cutt.us/DtS4E>
3. Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: <https://cutt.us/TvLAe>

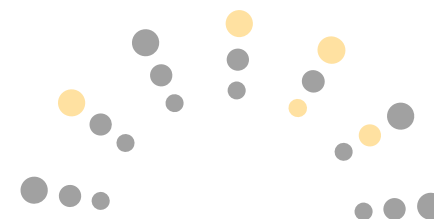


الفصل الثاني

كيفية تنفيذ عمليات الاحتيال عبر الإنترنت

- أولاً: الثغرات المُساعدة على عمليات الاحتيال عبر الإنترنت
- ثانياً: أمن البيانات الشخصية والاحتيال عبر الإنترنت
- ثالثاً: البصمة الرقمية والاحتيال عبر الإنترنت

0 2



أولاً: الثغرات المُساعدة على عمليات الاختيال عبر الإنترنت



تُعَدُّ الثَّغَرَاتُ الرَّقْمِيَّةُ من العوامل المُساعدة في الوقوع ضحية للاختيال عبر الإنترنت، وتُعرَف الثَّغرة الرَّقْمِيَّة على أنَّها مُصطلح يُطلق على مناطق ضعيفة في أنظمة تشغيل الحاسوب، هذه المناطق الضعيفة يمكن التَّسَلُّلِ عَبرها إلى داخل نظام التَّشغيل، ومن ثَمَّ يَتِمُّ التَّعْدِيلُ فيه لتدميره نهائياً، أو للتَّجسُّس على المعلومات الخاصة بِصاحب الحاسوب المُخْتَرَق، أو ما يُعرَف بجهاز الضَّحية⁽¹⁾؛ كما تظهر الثَّغرات الأُمْنِيَّة في جميع البرامج أيضًا وليس في أنظمة التَّشغيل فقط، وهي بسبب أخطاء بَرْمَجِيَّة أثناء تطويرها ارتكبتها المُطَوَّرُونَ، وتُشكِّلُ خطراً أُمْنِيًّا بسبب عدم اكتشافها في أغلب الأحيان ممَّا يَسْتَلْزَمُ إصداراً جديداً لإيجاد حلٍّ لها، ويُطلق عليها هنا الثَّغرات غير المكتشفة Zero-day التي دائماً ما يستعين بها القراصنة في جرائمهم الإلكترونيَّة. وثَّغرة Zero-day واحدة من هذه العيوب، وهي ثَّغرة في البرامج يُمكن استغلالها مِنْ قَبْلِ المُتَسَلِّلِينَ الذين ليس لديهم تصريح حتَّى الآن، حيث لا يَعْرِفُ مُطَوَّرُو البرامج مكان الضَّعف أو يُطَوَّرُونَ إصلاحاً له، أو أنَّهم يتجاهلون ذلك، وتؤدي هذه الثَّغرة الأُمْنِيَّة إلى خرقٍ خطير للأمن السَّيبراني⁽²⁾.

1. What is bug? Neterich. On site: <https://netenrich.com/glossary/bug>
2. What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: <https://cutt.us/FXNvU>

آلية الهجمات غير المكتشفة Zero-day

غالبًا ما تتم هجمات Zero-day وفقًا لعددٍ من المراحل المتسلسلة والمتعاقبة، وفيما يلي تبيان لهذه المراحل وفقًا لتسلسلها المنطقي والإجرائي:

البحث عن الثغرات الأمنية:

وهي الخطوة الأولى، وفيها يقوم المهاجمون بالبحث عن الثغرات الأمنية من خلال التعليمات البرمجية أو تجربة التطبيقات الشائعة، ويمكنهم أيضًا شراء نقاط الضعف من السوق السوداء⁽¹⁾.

إنشاء رمز الاستغلال:

يُنشئ المهاجمون برنامجًا ضارًا أو وسائل تقنية أخرى لاستغلال تلك الثغرة الأمنية.

البحث عن الأنظمة المتأثرة بالثغرة الأمنية:

يمكن للمهاجمين أن يستخدموا الروبوتات والماسحات الآلية وطرقًا أخرى لتحديد الأنظمة التي تعاني من الثغرة الأمنية.

التخطيط للهجوم:

في هجومٍ موجهٍ على أفراد أو مؤسسات معينة يقوم المهاجمون باستطلاعٍ مُفصّلٍ لتحديد أفضل طريقة لاختراق النظام الضعيف، ففي الهجوم غير المستهدف يستخدم المهاجمون عادةً برامج الروبوت أو حملات التصيد الاحتيالي الضخمة لمحاولة اختراق أكبر عددٍ ممكنٍ من الأنظمة المعرضة للخطر.

التسلل:

يخترق المهاجم أجهزة الأفراد أو المؤسسات.

إطلاق هجوم Zero-Day:

بعد الخطوات السابقة يبدأ المهاجم في تنفيذ التعليمات البرمجية عن بُعدٍ على الجهاز المُخترق.

1. How to Handle Zero-day, Nordic Defender, 2022. On site: <https://cutt.us/gUQ7g>

أمثلة على هجمات Zero-Day

فيما يلي أمثلة على هجمات الثغرة الأمنية التي تكشف عن مخاطر هذه الهجمات على المؤسسات والأفراد.

سوني Sony:

في عام 2014م، استهدف هُجوم Zero-Day شركة Sony Pictures، وأدى الهجوم إلى تدمير الشبكة الداخلية للشركة، وتسريب بيانات الشركة الحساسة على مواقع مشاركة الملفات، بما في ذلك المعلومات الشخصية حول موظفي Sony وعائلاتهم، والمراسلات الداخلية، ومعلومات حول رواتب المديرين التنفيذيين، ونسخ من أفلام سوني التي لم يتم طرحتها، وفي هذا الهجوم استخدم المهاجمون نوعًا مختلفًا من البرمجيات الضارة لمحو أنظمة متعددة على شبكة الشركة⁽¹⁾.

هجوم WannaCry:

تسبب هذا الهجوم في تعطيل أكثر من 200,000 جهاز في يوم واحد بجميع أنحاء العالم في مايو 2017م، وقد انتشر هجوم برنامج الفدية هذا عبر أجهزة الحاسوب التي تعمل بنظام التشغيل Microsoft Windows؛ حيث تمت السيطرة على ملفات المستخدمين وطلب فدية بعملة

Bitcoin لإعادتها؛ والسبب في هذا الهجوم هو استمرار العمل بأنظمة أجهزة الحاسوب القديمة غير المحدثة، فقد استغل المجرمون الإلكترونيون المسؤولون عن الهجوم نقطة ضعف موجودة في نظام التشغيل Micro-soft Windows باستخدام هجمة تسلل عُرفت باسم Eternal Blue.

فقبل شهرين من الهجوم كانت مايكروسوفت Microsoft قد أصدرت تصريحًا أمنيًا لحماية أنظمة المستخدمين، لكن مع عدم قيام الكثير من الأفراد بتحديث أنظمة التشغيل الخاصة بهم بانتظام كانوا الأكثر استهدافًا في هذا الهجوم؛ وقد طلب المتسللون عملة بيتكوين الرقمية bitcoin بقيمة 300 دولار، ثم رفعوا قيمة الفدية إلى 600 دولار لكل فرد، مقابل إعادة ملفات المستخدمين⁽²⁾.

الهجمات غير المكتشفة لثغرة Zero-day

لا بد من الإشارة هنا إلى نوع في غاية الأهمية لنا كأفراد؛ هو الهجمات غير المكتشفة لثغرة Zero-day، فعادةً ما يتم شن هجمات Zero-day غير المكتشفة ضد عدد كبير من مستخدمي المنزل (الأفراد العاديين) الذين يستخدمون نظامًا ضعيفًا، مثل نظام التشغيل أو المتصفح، وغالبًا ما يكون هدف المهاجم هو اختراق هذه الأنظمة واستخدامها لبناء شبكات روبوت ضخمة لتنفيذ جرائم إلكترونية أكبر فيما بعد⁽³⁾.

1. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: <https://cutt.us/ZwCye>
2. What was the WannaCry ransomware attack? cloudflare. On site: <https://cutt.us/8jM6q>
3. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: <https://cutt.us/Tr7jj>

ثانيًا: أمن البيانات الشخصية والاحتيال عبر الإنترنت

أخرى لصالح أنفسهم؛ ونشير هنا إلى أن كلمة "سرقة" في مُصطلح عالم الإنترنت لا تعني حرفيًا أخذ معلومات بعيدًا عن الضحية أو نزعها منه، بل ما يحدث عند سرقة البيانات هو أن المهاجم بكل بساطة ينسخ المعلومات كي يستخدمها هو بنفسه. ويُطلق على هذه الجريمة الإلكترونية مُصطلح "انتهاك البيانات" أو "تسرّب البيانات".

والشكل الأكثر شيوعًا من هذا النوع من الجرائم هو التّصيد الاحتيالي، ويحدث عندما يتنكر مُحتال في هيئة جهة موثوقة لخداع الضحية وجعله يفتح رسالة بريد إلكتروني أو رسالة نصية أو رسالة فورية تحتوي على تطبيق خبيث، والأشخاص الذين يقعون ضحية لهجمات التّصيد الاحتيالي يتعرضون لسرقة الهوية.

كما يمكن للأشخاص التّسبب في تعرّضهم للاحتيال عبر الإنترنت بأنفسهم عن طريق تنزيل برامج أو بيانات من مواقع إلكترونية مُختَرقة مُصابة بفيروسات مثل الفيروسات المُتَنقلة أو البرمجيات الضارة، ممّا يُعطى للمُجرمين إمكانية وصول غير مُصرّح به إلى أجهزتهم؛ ويُتيح لهم سرقة البيانات.

يُشير أمان المعلومات إلى مجموعة من الإجراءات والأدوات الأمنية التي تحمي على نطاق واسع المعلومات الحساسة من سوء الاستخدام أو الوصول غير المُصرّح به أو التّعطيل أو الإثلاف. ويشمل أمان المعلومات الأمن المادي والبيئي، والتّحكم في الوصول والأمان عبر الإنترنت⁽¹⁾.

أما سرقة البيانات، فهي عملية سرقة معلومات رقمية مُخزّنة على أجهزة الحاسوب أو الهواتف للحصول على معلومات سرّية أو انتهاك الخصوصية. ويمكن أن تكون البيانات المسروقة أي شيء مثل: معلومات الحساب المصرفي، وكلمات المرور على الإنترنت، ورّفم جواز السّفر، والسّجلات الطبية والاشتراكات عبر الإنترنت... وما إلى ذلك. وبمجرد وصول شخص غير مُصرّح له إلى معلومات شخصية يمكنه حذفها أو تغييرها أو منع الوصول إليها بدون إذن المالك⁽²⁾.

وتحدث سرقة البيانات عادةً بسبب رغبة أشخاص في بيع المعلومات أو استخدامها في سرقة الهوية. وإذا تمكّن لُصوص البيانات من سرقة معلومات كافية، يمكنهم استخدامها للوصول إلى حسابات آمنة أو إصدار بطاقات ائتمان باستخدام اسم الضحية أو استخدام هوية الضحية بطريقة

1. ما هو أمان المعلومات؟، مايكروسوفت. مُتاح على الرّابط: <https://cutt.us/CxorE>

2. ما المقصود بسرقة البيانات وكيفية منعها؟، Kaspersky. مُتاح على الرّابط: <https://cutt.us/Ve2to>

ثالثاً: البصمة الرقمية والاحتيايل عبر الإنترنت



يُشير مُصطلح "البصمة الرقمية" أو الظل الرقميّ أو البصمة الإلكترونية، إلى أثر البيانات التي تُتركها عند استخدام الإنترنت، وهي تشمل مواقع الويب التي تزورها، ورسائل البريد الإلكتروني التي تُرسلها وتُستقبلها، والمعلومات التي تُقدّمها عبر الإنترنت⁽¹⁾.

ويمكن استخدام البصمة الرقمية (أو الإلكترونية) لمتابعة أنشطة أي شخص على الإنترنت وأجهزته؛ على سبيل المثال، ما يقوم به الشخص من نشر على وسائل التواصل الاجتماعي أو الاشتراك في رسالة إخبارية أو ترك مراجعة على الإنترنت أو التسوق عبر الإنترنت، كلّها أنشطة تُشكّل "البصمة الرقمية". كما يمكن لمواقع الإنترنت تتبع نشاط الزائرين عن طريق تثبيت ملفات تعريف الارتباط على جهازهم، ويمكن للتطبيقات تجميع بيانات المستخدمين أيضاً من دون علمهم بذلك؛ ويتم ذلك بمجرد أن تسمح لمؤسسة ما بالوصول إلى معلوماتك، فعندئذ يمكنها بيع بياناتك إلى جهات خارجية أو مشاركتها معها، والأسوأ من ذلك أنه قد يتم كشف سرية معلوماتك الشخصية في إطار انتهاك البيانات.

1. What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: <https://cutt.us/teSUS>

أنواع البصمة الرقمية

هناك نوعان من البصمات الرقمية؛ أحدهما نشط، والآخر غير نشط؛ وفيما يلي تبيان لكلا النوعين:

البصمات الرقمية النشطة

فهذه عملية خفية قد لا يدرك المستخدمون حدوثها. وكذلك يمكن أن تتشكل تلك البصمة من خلال مواقع الإنترنت التي تتصفحها، واهتماماتك عبر شبكات التواصل الاجتماعي، وعمليات البحث التي تجريها في إنشاء ملفك الشخصي، ويستفيد المقلون من عمليات إبداء الإعجاب والمشاركة والتعليقات لتكوين انطباعات عن اهتماماتك الشخصية، واستهدافك بمحتوى محدد⁽¹⁾.



يُقصد بها مشاركة المستخدم معلومات عن نفسه عمداً، فمثلاً من خلال النشر أو المشاركة على مواقع شبكات التواصل الاجتماعي أو المنتديات عبر الإنترنت. أو إذا قام مستخدم بتسجيل الدخول إلى موقع ويب باسم مستخدم أو ملف تعريف مسجل، فإن أي منشورات يقوم بنشرها تشكل جزءاً من بصمته الرقمية النشطة.

وكذلك عمليات ملء نموذج عبر الإنترنت، للاشتراك في رسالة إخبارية أو الموافقة على قبول ملفات تعريف الارتباط في متصفحك كلها تشكل بصمة الفرد الرقمية النشطة.

البصمات الرقمية غير النشطة (السلبية)

يتم إنشاء البصمة الرقمية غير النشطة عندما يتم جمع معلومات حول المستخدم دون أن يدرك أن هذا يحدث. على سبيل المثال، يتم ذلك عندما تجمع مواقع الويب معلومات حول عدد مرات زيارة المستخدم لها، والموقع الذي يدخل منه، وعنوان IP الخاص به.

1. حمادي، خالد. البصمة الرقمية... الظل الإلكتروني الخفي، جامعة العربي التبسي تبسة، الجزائر، يوليو 2021م، متاح على الرابط: <https://cutt.us/QToSN>

الآثار السلبية للبصمة الرقمية

قد تؤدي البصمات الرقمية إلى أضرار ونتائج سلبية بالنسبة لمستخدمي الإنترنت، وهذه الأضرار لا يمكن أن تحدث ما لم يكن هناك أخطاء من قبل المستخدم، وفيما يلي تبيان لأهم الآثار السلبية التي من الممكن أن تسببها البصمات الرقمية:

01

تُعد بيانات دائمة نسبياً،
وتُصبح متاحة للاطلاع العام أو الجزئي،
كما هو الحال مع منشورات Facebook
وبقية التطبيقات الاجتماعية، تُصبح
سيطرة المالك على كيفية استخدام
الآخرين لها ضعيفة.

02

يُمكن للبصمة الرقمية أن تُحدد
سمعة الشخص، كما هو الحال على
أرض الواقع.

03

يُمكن إساءة تفسير الكلمات والصور
التي ينشرها الفرد عبر الإنترنت أو
تغييرها، مما يتسبب في إهانة غير
مقصودة.

04

يُمكن للمحتوى المُخصَّص
لمجموعة خاصة أن ينتشر خارجها،
الأمر الذي قد يضرّ بالعلاقات بين
الأفراد.

05

يستطيع مجرمو الإنترنت
استغلال بصمتك الرقمية لأغراض
مثل الانتحال عبر الإنترنت للوصول
إلى الحساب أو إنشاء هويات مُزيفة
بناءً على بياناتك الشخصية وخداع
الآخرين.

أمثلة على البصمة الرقمية

01

التسوق عبر الإنترنت.

02

عمليات شراء من مواقع التجارة الإلكترونية.

03

التسجيل لإنشاء حساب على موقع ويب مُعَيَّن.

04

تنزيل تطبيقات التسوق واستخدامها.

05

التسجيل من أجل النشرات الإخبارية للعلامات التجارية.

06

الخدمات البنكية عبر الإنترنت.

07

استخدام تطبيق الخدمات المصرفية للهاتف المحمول.

08

الاشتراك في المطبوعات والمُدونات.

09

فَتَحْ حِسابَ بَطاقة ائتمان.

10

اسْتِخدام وسائل التَّواصل
الاجتماعيَّ على الأجهزة
الخاصَّة بك.

11

تسجيل الدُّخول إلى
مواقع الويب الأخرى
باستخدام بيانات اعتماد
وسائل التَّواصل الاجتماعيَّ.

12

التَّواصل مع الأصدقاء
وجهات الاتِّصال عَبر
الإنترنت.

13

مُشارَكة المعلومات
والبيانات والصُّور مع
معارفك.

14

الاشتراك في مصدرٍ إخباريٍّ
عَبر الإنترنت.

15

إعادة نَشْر المعلومات
التي تقرؤها.

16

استخدام أجهزة تتبَّع اللياقة
البدنيَّة.

حماية البصمة الرقمية

فيما يلي بعض النصائح لحماية البيانات الشخصية وإدارة السمعة الشخصية للأفراد عبر الإنترنت:

التحقق من البصمة الرقمية عبر مُحركات البحث

يمكن للفرد عبر إدخال اسمه في مُحركات البحث، مراجعة نتائج مُحرك البحث والمعلومات المتاحة عنه للاطلاع العام. فإذا كانت أي من النتائج تظهره بمظهر سلبي، يمكنه الاتصال بمسؤول الموقع لمعرفة ما إذا كان بإمكانه إزالتها أم لا؛ ويُعدّ إعداد تنبيهات Google إحدى طرق مراقبة اسم المُستخدم⁽¹⁾.

تقليل عدد مصادر المعلومات

تحتوي مواقع الويب على معلومات أكثر مما قد يرغب الفرد في عرضه. وغالبًا ما تتضمن هذه المواقع معلومات شخصية، مثل رقم الهاتف والعنوان والعمر، لذا على الفرد إزالة المعلومات الشخصية من هذه المواقع الإلكترونية أولًا بأول.

تقييد كمية البيانات التي يتم مشاركتها

في كل مرة تُقدّم فيها معلومات شخصية لمؤسسة ما، فإننا نمنع بصمتنا الرقمية، كما أننا نزيد من احتمالية قيام إحدى المؤسسات التي تُخزن

بياناتنا بإساءة استخدامها أو تعرضها للانتهاك، ما يضع بياناتنا بين الأيدي الخطأ؛ وبناءً على ذلك، علينا التفكير جيدًا قبل تقديم أي معلومات لأي جهة على الإنترنت.

التحقق من إعدادات الخصوصية

تسمح إعدادات الخصوصية على وسائل التواصل الاجتماعي بالتحكم في من يرى منشوراتنا. لذا يُفضّل مراجعة هذه الإعدادات، والتأكد من ضبطها على المستوى الذي نأسبنا. فمثلًا يتيح Facebook قسّ المشاركات على الأصدقاء، وإنشاء قوائم مُخصصة بالأشخاص الذين يمكنهم مشاهدة منشورات مُعينة.

التفكير جيدًا قبل مشاركة معلوماتنا على وسائل التواصل الاجتماعي

تُسهّل وسائل التواصل الاجتماعي الاتصال بالآخرين، ولكن يمكنها أيضًا أن تُسهّل الإفراط في مشاركة المعلومات الشخصية عليها، لذا يجب التفكير جيدًا قبل الكشف عن موقعنا أو أي معلومات شخصية أخرى مثل رقم الهاتف أو عنوان البريد الإلكتروني.

1. How to protect your digital footprint, state farm, 2023. On site: <https://cutt.us/OcHUG>

تجنب المواقع غير الآمنة

يجب علينا أثناء تصفح الإنترنت التأكد من أننا نتعامل مع موقع ويب آمن يبدأ عنوان URL بـ https:// وليس http:// - ؛ حيث يشير حرف "s" إلى اللفظ "آمن". ويجب أن يكون هناك أيضًا رمز قفل على يسار شريط العنوان.

الحذر عند استخدام شبكة Wi-Fi العامة

تعدّ شبكة Wi-Fi العامة بطبيعتها أقلّ أمانًا من الشبكة الشخصية؛ لأننا لا نعرف من قام بإعدادها أو من قد يشاهدها أيضًا. لذا ينبغي تجنب إرسال معلومات شخصية عند استخدام شبكات Wi-Fi العامة.

حذف الحسابات القديمة

تتمثل إحدى طرق تقليل بصمتنا الرقمية على الإنترنت في حذف الحسابات القديمة، ومن ذلك، على سبيل المثال، الملفات الشخصية في وسائل التواصل الاجتماعي التي لم نعد نستخدمها أو اشتراكات الرسائل الإخبارية.

كتابة كلمات مرور قوية وتغييرها من حين إلى آخر واستخدام Password Manager

يجب أن تكون كلمة المرور القوية طويلة، أي تتكوّن من 12 حرفًا على الأقل، والأمثل أن تكون أكثر من ذلك، وتحتوي على مزيج من الأحرف

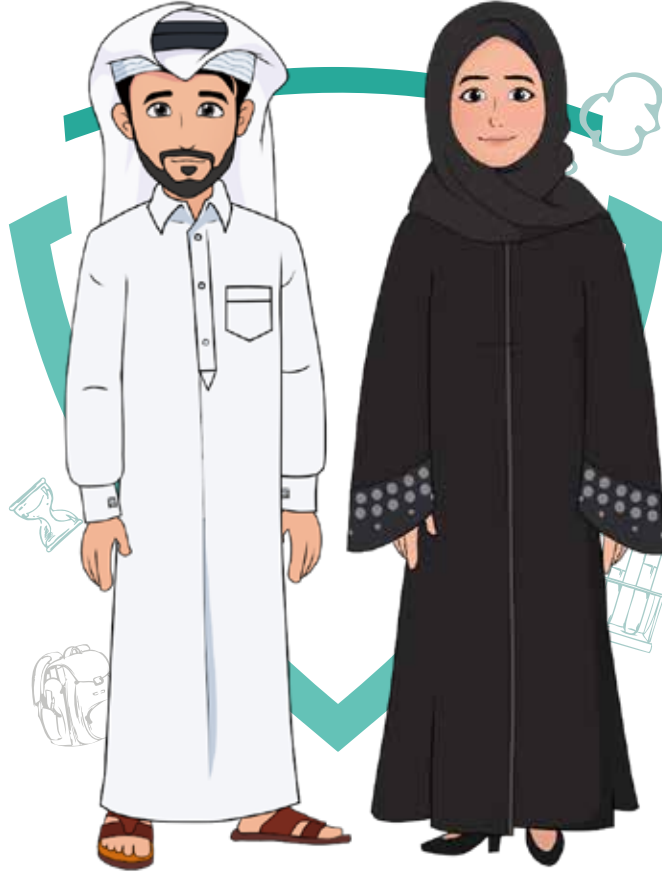
الكبيرة والصغيرة، بالإضافة إلى الرموز والأرقام. وكلّما كانت كلمة المرور أكثر تعقيدًا وصعوبة، أصبح اختراقها أصعب؛ ويساعد استخدام Password Manager على إنشاء جميع كلمات المرور الخاصة بنا وتخزينها وإدارتها في حساب عبر الإنترنت واحد آمن.

عدم تسجيل الدخول باستخدام Facebook

يُعدّ تسجيل الدخول إلى مواقع الويب والتطبيقات باستخدام Facebook أمرًا سهلًا. لكننا، في كلّ مرّة نقوم فيها بتسجيل الدخول إلى موقع ويب تابع لجهة خارجية باستخدام بيانات اعتماد Facebook الخاصة بنا، نمنح هذه الشركة الإذن للاطلاع والاحتفاظ ببياناتنا الخاصة، ممّا قد يُعرض معلوماتنا الشخصية للخطر.

تحديث البرامج باستمرار

يمكن أن تحتوي البرامج القديمة على العديد من البصمات الرقمية. ومن دون آخر التحديثات، يمكن لمجرمي الإنترنت الوصول إلى هذه المعلومات. قممرو الإنترنت قادرون على الوصول بسهولة إلى أجهزة وبيانات الضحية من خلال استغلال الثغرات في البرامج. والحلّ يكمن في تحديث البرامج باستمرار؛ فقد تكون البرامج الأقدم أكثر عرضة لهجمات المتسللين.



تعيين كلمة مرور للهاتف المحمول

قُم بتعيين رمز مرور لجهاز المحمول؛ حتى لا يتمكن الآخرون من الوصول إليه في حال فقده. وعند تثبيت تطبيق، اقرأ اتفاقية المستخدم؛ لأن العديد من التطبيقات تكشف عن نوع المعلومات التي تجمعها، وما قد تستخدم من أجله. وقد تقوم هذه التطبيقات بحفظ البيانات الشخصية، مثل البريد الإلكتروني والموقع والأنشطة عبر الإنترنت.

التحرك بسرعة بعد انتهاك البيانات

في حال الشك بانتهاك البيانات الخاصة بنا يجب التحرك فوراً، خاصة إذا كان الأمر يشمل خسارة مالية، وأولى الخطوات هي تغيير أي كلمات مرور ربما تم كشفها. وإذا كنت قد استخدمت كلمة المرور ذاتها لحسابات أخرى، فقم بتحديثها في جميع الحسابات⁽¹⁾.

1. How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: <https://cutt.us/G7awc>

الفصل الثالث

كيفية التصرف في حال التعرض للاختيال عبر الإنترنت

- أولاً: إرشادات الحماية من الاختيال عبر الإنترنت
- ثانياً: حماية البيانات من الاختيال عبر الإنترنت
- ثالثاً: الجهات التي ألجأ إليها عند تعرضي للاختيال عبر الإنترنت



أولاً: إرشادات الحماية من الاحتيال عبر الإنترنت

الحذر من المعاملات التي تتضمن أطرافاً مجهولة

يجب الحذر عند طلب استقبال أي تحويلات مالية ثم تحويلها إلى طرفي ثالث، فقد يكون ذلك عملية نصب أو غسيل أموال.

الاستعانة ببرامج مكافحة الفيروسات

سواءً على الهاتف الذكي أو جهاز الحاسوب، يجب تثبيت مكافحة فيروسات معروف، ويحظى بسُمعة جيدة؛ من أجل تعزيز مستوى الحماية على الأجهزة الخاصة.

استخدام كلمات مرور معقدة وتغييرها من حين إلى آخر

يفضل أن تتضمن حروفاً ورموزاً وأرقاماً، كما يجب تغييرها فوراً كلما أدركت أن هناك ما يدعو للشك.

عدم التسوق من المواقع المجهولة

لا تقم بأي عملية شراء عبر الإنترنت إلا من المواقع المشهورة والمتاجر الإلكترونية ذات السمعة الطيبة، وإن راودك بعض الشك حول مصداقية بعض المواقع، فینبغی البحث عنها أكثر للتأكد من وضعها.

يبتكر المُحتالون طرقاً وآليات جديدة لتنفيذ جرائمهم الإلكترونية، غير أن اتخاذ بعض الإجراءات البسيطة كفيل بتعزيز أمن المعلومات، وفيما يلي تبيان لأهمها:

تحميل التطبيقات من المتاجر المعروفة

ينبغي تحميل كل التطبيقات من المتاجر المعروفة، فعملية تحميل أي تطبيق من مصادر مجهولة قد تُعرض البيانات والخصوصية للسرقة، مما يعني التعرض لنوع من الابتزاز والاحتيال عبر الإنترنت.

تحديث تطبيقات الهاتف

لا بد من تثبيت التحديثات الجديدة الخاصة بنظام الهاتف، فهي دائماً تتضمن ملفات تُعزز من حماية الهاتف من أشكال الاختراق المختلفة.

تجنب الروابط مجهولة المصدر

حتى ولو أرسلت من الأصدقاء، فبمجرد الضغط عليها قد تتعرض للاختراق، أو تثبيت برمجيات خبيثة على هاتفك دون معرفتك، وكذلك لا تفتح رسائل البريد الإلكتروني المجهولة.

ثانيًا: حماية البيانات من الاحتيال عبر الإنترنت

- إن حماية البيانات الشخصية والمالية من الاحتيال أمر ممكن، ويمكن تحقيق هذه الحماية من خلال عدة إجراءات، فيما يلي تبيان لأهمها:
- التيقظ لعمليات الاحتيال عند التعامل مع اتصالات متطفلة من قبل أشخاص أو أي جهة؛ سواء كانت عبر الهاتف، البريد، الرسالة الإلكترونية، أو على موقع لشبكات التواصل الاجتماعي، فقد تكون عملية احتيال.
- إذا أجريت مُحادثة مع شخص ما عبر الإنترنت، عليك أخذ الوقت الكافي للبحث عنه، مثل البحث عن الصور في محرك Google للصور، أو البحث عبر الإنترنت عن أشخاص آخرين من المحتمل أن يكونوا قد تعاملوا معه.
- لا تفتح نصوصًا أو نوافذ تظهر أمامك أو رسائل إلكترونية غير موثوقة مع ضرورة التأكد من هوية المتصل عبر مصدرٍ مُستقلٍّ مثل البحث على الإنترنت.
- احتفظ بتفاصيلك الشخصية بشكلٍ آمنٍ، مثل وضع قفل على صندوق بريدك، مع الاحتفاظ بكلمات السر والأرقام السرية الخاصة بك في مكانٍ آمنٍ، مع الحذر من المعلومات الشخصية التي تُشارك بها على مواقع التواصل الاجتماعي.
- تحديث أنظمة أجهزة هاتفك والحاسوب الخاص بك باستمرار، والاحتفاظ بنسخة احتياطية للمحتوى.
- ضع كلمة سر لشبكتك الخاصة بال-Wi-Fi وتفاذي استخدام أجهزة حاسوب عامة أو النقاط الساخنة في ال-Wi-Fi.
- راجع ترتيباتك المتعلقة بالخصوصية والأمن على مواقع التواصل الاجتماعي.
- احذر من أي طلبات تتعلق بتفاصيلك أو مالك.
- كن حذرًا عندما تتسوق على الإنترنت، وخاصة العروض التي تبدو مغرية جدًا.
- عند مراجعة نبذة تعارف جديدة، لاحظ أي شيء غير عادي في خيارات الشخص الآخر مثل: (الصورة، أو المكان، أو الاهتمامات، أو تطابق المهارات اللغوية مع الخلفية)؛ فغالبًا ما يستعمل المحتالون صورًا مزورة وجذوها على الإنترنت. لذا فم بعملية بحث عن صورة الشخص المُعجب بك لمساعدتك على التثبت من أنه فعلاً الشخص الذي يقول إنه هو، ويمكن الاستعانة بخدمات البحث عن الصور مثل Google.

- غَيَّر كلمات السرّ الخاصّة بك على الإنترنت: إذا كنت تعتقد بأنّ الحاسوب الخاصّ بك أو الهاتف قد تعرّض للقرصنة، فيجب إجراء فحصٍ شاملٍ لنظامك الإلكترونيّ بواسطة الفيروسات المُقْتَدَة، ثمّ قُمْ بتغيير كلمة السرّ. وكذلك الأمر بالنسبة للحسابات على الإنترنت، سواءً على مواقع التواصل الاجتماعيّ أو مواقع التسوّق وغيرها.
- ضَع إشارة مرجعيّة للمواقع المهمّة، عبْر إضافة جميع المواقع التي تقوم بزيارتها باستمرارٍ إلى الإشارات المرجعيّة الخاصّة بك، وافتحها فقط من هناك، وبهذا تقيضي على خطر فتح صفحاتٍ وهميّةٍ بطريق الخطأ.
- هناك عدّة علامات تحذيريّة لاكتشاف الوثائق المُروّرة؛ مثل "بيانات الحسابات المصرفيّة" أو "رحلات الطّيران" التي قد تكون فخاً من قِبَل المُتسلّلين في صورة هدايا وهميّةٍ لمعرفة البيانات الشخصيّة من الأفراد، مثل: التّحيّات العامّة بدلاً من التّحيّات الشخصيّة، استخدام أسماء مُنظّمة غير موجودة، ركاكة في المظهر، ضَعف في القواعد والتّهجئة، مُبالغة في الرّسميّات.

تذكّر أنّ رسائل الخطأ الحقيقيّة من Microsoft أو شركات تقنيّة كبيرة

1. احم نفسك من عمليّات الاختيال والهجمات عبْر الإنترنت، مايكروسوفت. مُتاح على الرّابط: <https://cutt.us/YVxY1>

أخرى، لا تتضمّن أبداً أرقام هواتف لكي تتّصل بها.

- لن تتّصل بك مايكروسوفت Microsoft وشركات التّقنيّة الأخرى أبداً ليُخْبِرَكَ بأنّ هناك مشكلة في جهازك. ما لم تتّصل بهم أوّلاً، لن يحتاج وكلاء الدّعم التّقنيّ أبداً إلى أن يطلبوا منك رقم الضّمان الاجتماعيّ الخاصّ بك أو أيّ معلوماتٍ شخصيّةٍ أخرى غير مُرتبطة. إذا حصلت على مُكالمة من شخصٍ ما يَعرِض دَعماً تقنيّاً غير مرغوب فيه، فقم بإنهاء المكالمة معه.
- إذا كانت شاشتك تمتلئ بشكّلٍ مُفاجئٍ بالتّوافذ المُنبثقة المُخيفة؛ يجب إغلاق المُستعرض على الفور (حاول الضّغط على ALT+F4 إذا لم تتمكّن من القيام بذلك باستخدام الماوس)، وإذا لم تتمكّن من إغلاق المُستعرض، فحاول إعادة تشغيل الحاسوب⁽¹⁾.

ثالثاً: الجهات التي ألجأ إليها عند تعرّضي للاحتيال عبر الإنترنت

كما ينبغي على المُستهدف عدم تصديق ما يقوله المُتسلّل أو أن يترك مجالاً له للتلاعب بأعصابه.

وأخيراً، إنَّ أيَّ معلوماتٍ تعرفها أو رقم يخص هذا المُتسلّل أو أيَّ رسائل أرسلت إليك، ينبغي عليك تقديمها إلى أشخاص محلّ ثقة ليتمكّنوا من تقديمها إلى إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية في دولة قطر.

في حالة التّعرّض لجريمة احتيالٍ إلكتروني، فلا يجب ترك الأمر للوقت، بل ينبغي التّحرّك فوراً منقاً لتفاهم الأزمة، فأولاً يجب عليك عدم التّواصل مع الشّخص المُحتال أو إعادة إرسال أيّ رسائل تشكّ في مصداقيّتها مُجدّداً، ثمّ أغلق جميع الحسابات المفتوحة وفتّ تلقّي الرّسالة التّحذيريّة أو الشّكّ بتعرّض أيّ من الحسابات للاختراق أو تلقّي رسالة تهديدٍ وابتزازٍ من مجهول، وكذلك إغلاق الأجهزة مع الاحتفاظ بنصّ الرّسالة المُرسّلة لكونها دليلاً يُدين المُتسلّل.

وهنا يجب إبلاغ شخصٍ تثق به، مثل الوالدين أو أحد المُشرفين في المدرسة؛ فهو أمرٌ ضروريٌّ لا ينبغي الخجل منه، فوفق الإحصائيات العالميّة هناك شخصٌ من بين 100 شخصٍ يتعرّض لواجِدٍ من جرائم الإنترنت، وفي مُقدّماتها التّزوير والاحتفال.

وعليك التّأكّد من عدم مُجاراة المُتسلّل؛ لأنّه شخصٌ مُحترّف في تهريب الآخرين لتحقيق الفَرْص الذي يسعى لإجازه من الاحتفال عليك، ولا ترضخ لطلّباته أيضاً مثل إرسال المال في حال طلبه منك بشكّلٍ مُباشرٍ كما يحدث في هجمات الفدية.

أمثلة على أشهر عمليات الاحتيال عبر الإنترنت

المثال الثاني: العملات الرقمية

في عام 2017م، خسر العديد من الأشخاص آلاف الدولارات بعد أن فقدوا عملات رقمية من نوع "إثيريوم"، حيث اخترق المهاجمون محفظة العملة، وقاموا بتحويلها نحو خادمتهم الخاصة⁽²⁾.

وفي العام نفسه (2017م) انتشر فيروس أطلق عليه "WannaCry" أو "هجوم طلب الفدية"، والذي تسبب في تعطل الحواسيب. ومن أجل استعادة إمكانية الدخول طالب المخترقون من أصحاب الأجهزة بدفع مبلغ من المال على شكل عملة (بيتكوين) لصقوبة اقتفاء أثرها، وبالتالي الهرب بفعلتهم دون عقاب⁽³⁾.

يعد أسلوب كسب ثقة الضحية، ثم الإقدام على سرقة أمواله وبياناته الخاصة هو الأكثر انتشارًا في عمليات التصيد الإلكتروني، فهنا يلجأ القراصنة إلى شن هجماتهم عبر البرمجيات الخبيثة، وغالبًا ما تنتهي هجمات الاحتيال عبر الإنترنت بعواقب وخيمة على الأفراد والشركات.

ومن أجل فهم خطورة الاحتيال عبر الإنترنت تعرض بعض أشهر الأمثلة التي وقعت في العالم:

المثال الأول: شركة تويوتا بوشوكو

في عام 2019م تعرضت شركة "تويوتا بوشوكو" التي تعمل على توريد وتزويد سيارات تويوتا بقطع المعدات لعملية اختيال إلكتروني بلغت قيمتها حوالي 37 مليون دولار أمريكي؛ إذ أقنع المختالون الإلكترونيون المدير المالي للشركة بتغيير معلومات الحساب المصرفي للمستلم، وهو ما ساعدهم على الحصول على هذه الأموال⁽¹⁾.

1. Toyota Boshoku Corporation loses \$37 million in Business Email Compromise scam, CYWARE SOCIAL. On site: <https://cutt.us/ffDMv>
2. '300m in cryptocurrency' accidentally lost forever due to bug, The Guardian. On site: <https://cutt.us/ILdpQ>
3. Ransomware News, Ransomware Timeline: Top Stories December 2017, Cyber defense magazine. On site: <https://cutt.us/IJBEQ>

المثال الثالث: شركة Yahoo

خلال الفترة الممتدة بين عامي 2013م - 2016م، تعرّضت شركة ياهو إلى سرقة بيانات حوالي 3 مليارات مُستخدم؛ حيث تمكّن المهاجمون من الوصول إلى معلومات وكلمات مرور يمكن استخدامها في الوصول إلى خدمات وحسابات أخرى على الإنترنت⁽¹⁾.

المثال الرابع: سرقة الأموال في روسيا

انتشر في روسيا بين عامي 2013م و2014م واحدٌ من أبرز أساليب الاحتيال عبر الإنترنت؛ حيث يقوم أحد المُحتالين بالاتصال بصحّته، ويتّحل شخصيّة مُوظّف في البنك الذي يتعامل معه المُستهدف، ويطلب منه معلومات تتعلّق بالبطاقة المصرفيّة بحجّة إيقاف مُعاملات ماليّة غير مشروعة وبغْد حصول المُحتال على بيانات البطاقة يقوم باستغلالها لسرقة وتحويل الأموال إلى حسابات تخصّه⁽²⁾.

المثال الخامس: سرقة 600 مليون دولار في عملية اختيال ضخمة بالعمّلات الرّقميّة

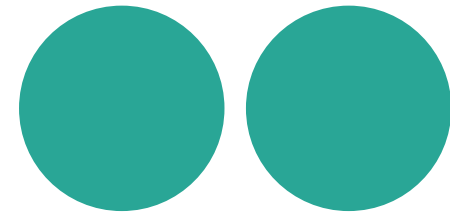
قام قراصنة إلكترونيّون بسرقة حوالي 600 مليون دولار، في واحدٍ من كبرى عمليّات الاختيال في تاريخ العمّلات الرّقميّة؛ وقد استغلّ القراصنة ثُغرةً أمنيّةً في نظامها لسرقة الأموال التي تعود لعشرات الآلاف من أعضاء مُجتمع الشّفير⁽³⁾.

1. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, The New York times. On site: <https://cutt.us/oOhv7>

2. أشهر طرق الاحتيال عبر الإنترنت التي انتشرت في السنوات الأخيرة، روسيا اليوم، 2020م. مُتاح على الرابط: <https://cutt.us/gDg5J>

3. القرصنة الإلكترونيّة: سرقة 600 مليون دولار في عمليّة اختيال ضخمة بالعمّلات الرّقميّة، بي بي سي عربي، 2021م. مُتاح على الرابط: <https://cutt.us/ToS7P>

تمارين وتذريّات



تَمَارِين وَتَدْرِيبَات

- تُعَدُّ التَّمارِين جزءًا رئيسًا من عملية التَّدريب، وهي تُحَقِّق عِدَّة أهدافٍ وغاياتٍ، فيما يلي تبيان لأهمِّها:
- التَّمارِين أداة فعَّالة لمعرفة مدى استِفادة الطَّلَبَة من المُحتَوَى التَّدريبيِّ، ومدى الأثر الذي حقَّقه على المَحْزُون المَعْرِفي لدى الطَّلَبَة.
- أداة مُهمَّة لترسيخ المعلومات والمعارِف لدى الطَّلَبَة؛ كونها تُمثِّل مُراجَعَة سريعة للمحتوى التَّدريبيِّ.
- اكتشاف الفُرُوق المعرفيَّة بين الطَّلَبَة.
- تُمثِّل تغذية عكسيَّة للمُدَرِّب، وتُقَدِّم له معلومات حول فاعليَّة الحَقِيبَة التَّدريبيَّة وفاعليَّة أسلوبه التَّدريبيِّ.
- خلال التَّدريب وبعد الانتهاء من فِكرَة ما، يطلب المُدَرِّب من الطَّلَبَة قَنَح الكُتَيْب الخاصِّ بهم، والإجابة عن السُّؤال المُحدَّد، والذي يرتبط بِشَكْلٍ مُباشر بالفِكرَة أو الموضوع الذي يُقدِّمه لهم.
- التَّمارِين مُختارة بِعناية؛ بحيث تكون مُبسَّطة وسَهلة الفَهم، وقابلة للحلِّ مِن قَبَل طَلَبَة المرحلة الإِعداديَّة، وهنا من المُمكن للمُدَرِّب تقديم الدَّعم للطَّلَبَة في الإجابة عن بعض التَّمارِين في حال اقتضت الصُّرورة، وهذا الأمر يُثَرِّك لتَقدير المُدَرِّب.
- التَّمارِين ستكون على جُزأين؛ جزء خاصِّ بالصِّفِّ، وتُسمَّى بالتَّمارِين الصِّفيَّة، وآخر لَاصِفيِّ، يقوم الطَّالِب بالإجابة عنها كواجبٍ مَنزليِّ.
- إضافة الحلِّ الخاصِّ بِكُلِّ تمرين، مع تمييز الإجابة بِلَوْنٍ مُختلِف.

وفيما يلي تبيان للتَّمارِين الخاصَّة بِطَلَبَة المرحلة الإِعداديَّة، مُرتَّبة وَفَقًا لطبيعتها الصِّفيَّة والَاصِفيَّة، مع العِلْم بأنَّ ذات التَّمارِين وبصيفتها الموجودة هنا هي ذاتها موجودة في الكُتَيْب الخاصِّ بالطَّالِب.

مَنْهَجِيَّة التَّعَامُل مع التَّمارِين

التَّمارِين المذكورة في هذا القِسم شاملة للمحتوى التَّدريبيِّ في هذه الحَقِيبَة، وفيما يلي توضيح للمَنْهَجِيَّة المُقترَحة للتَّعَامُل معها:

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.



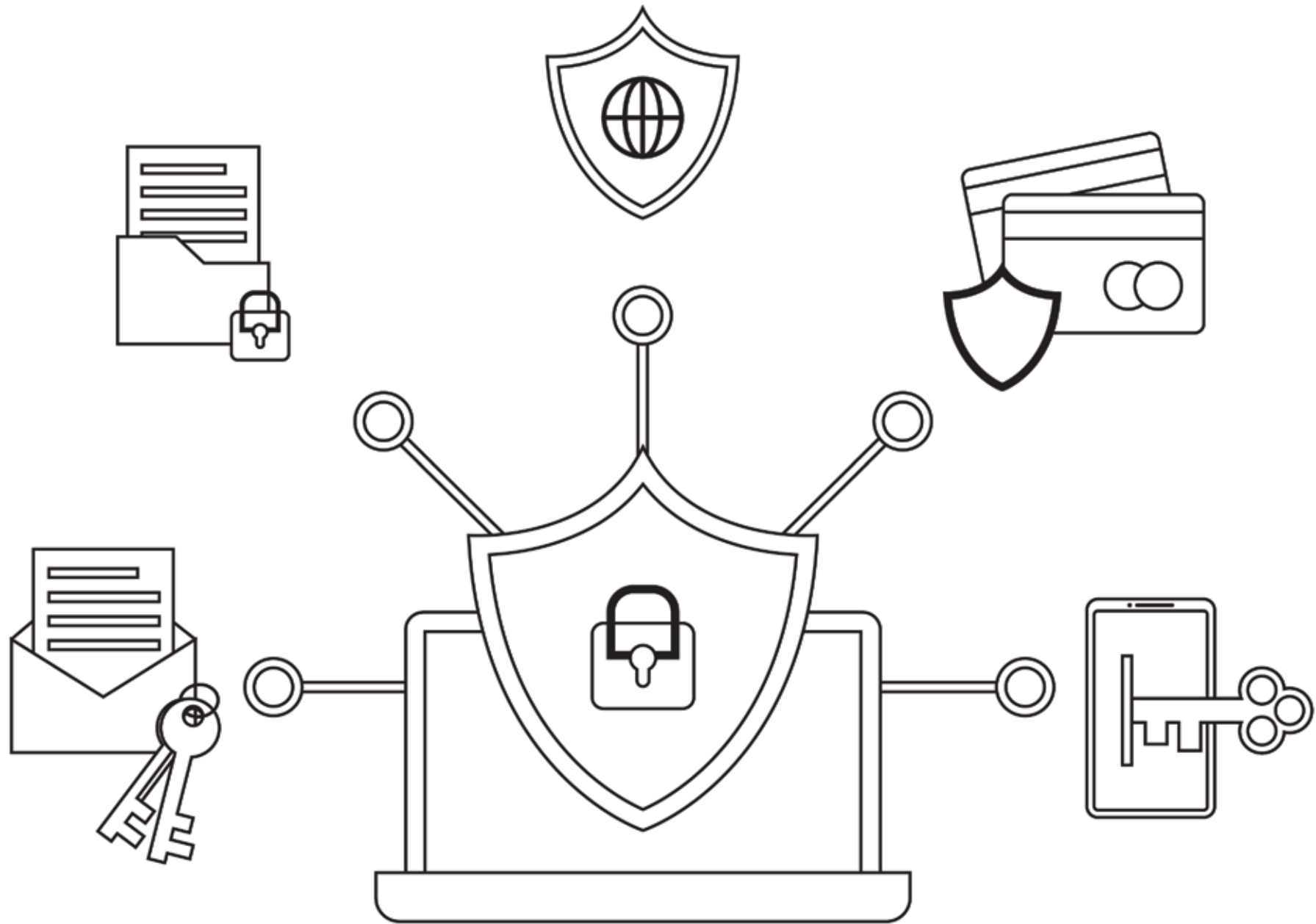
أولاً: التمارين الصفية

التدريبات هنا مُرفقة بالحل، بينما في كُتَيْب الطالب مَكْتُوبة بدون حل، ومُرفق معها توجيه للطالب لكيفية الحل، وذلك حيث تقتضي الضرورة.



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.



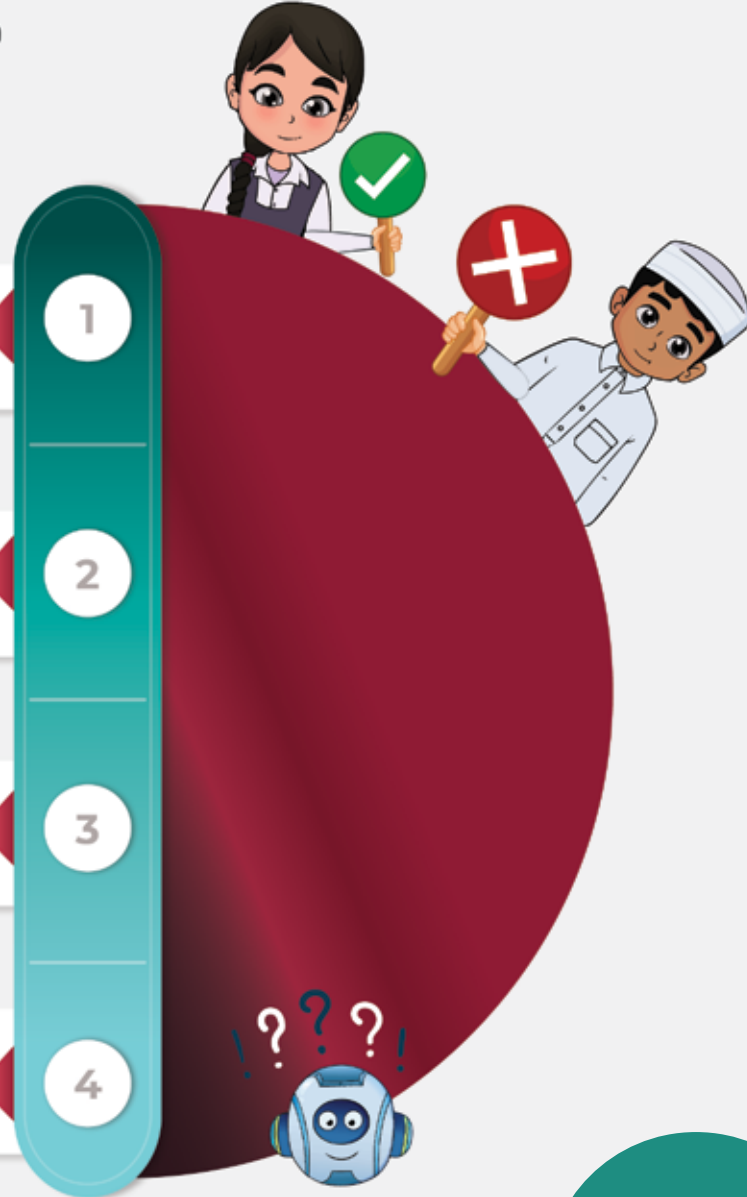
جريمة الاحتيال عبر الإنترنت هي الدّخول المُصرّح به من أجل الحصول على معلومات وبيانات موجودة على الحاسب الآلي.



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.





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



6 الاحتيال المعلوماتي هو الفِش والخداع المعلوماتي من خلال التَّلعب 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 تَلعب.

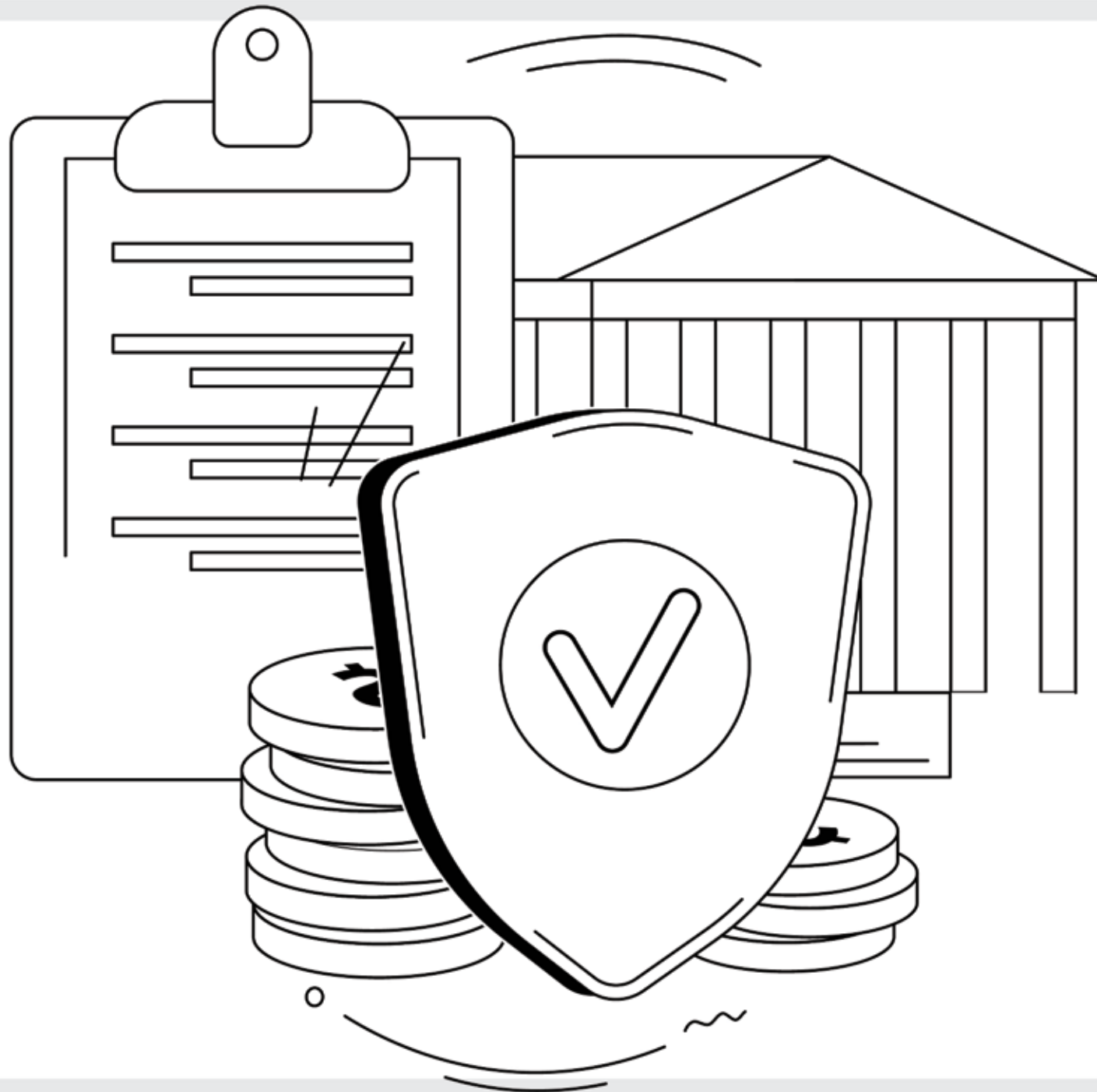


انتبه!

التَّصَبُّعُ عِبر الإنترنت

الاستيلاء على مال الآخرين بوسيلةٍ يَشُوْبهَا الخِداْع، ما يَتَسَبَّبُ فِي تَسَلُّمِ هَذَا الْمَالِ عَنْ طَرِيقِ أَجْهَزةِ الْحَاسُوبِ وَالْأَجْهَزةِ الذَّكِيَّةِ.





هل تعلم؟

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



التَّمرين الثاني

صِل المُصطلحات والعبارات من العمود (أ)
بما يناسبها من العمود (ب):

العمود (أ)

- ☐ الاحتيال عبر الرسائل النصية القصيرة
- ☐ الاحتيال عبر الإعلانات
- ☐ فيروسات الفدية
- ☐ الاحتيال بسرقة بطاقات الائتمان
- ☐ الاحتيال الصوتي
- ☐ احتيال التسوق عبر الإنترنت
- ☐ الاحتيال بجمع التبرعات
- ☐ الاحتيال على البائع عبر الإنترنت

العمود (ب)

- ☒ يتم إرسال رابط من خلال رسالة نصية، بمجرد الضغط عليها تتم عملية الاحتيال.
- ☒ الإعلانات الخبيثة المحملة بالفيروسات والتي تُستخدم في سرقة المعلومات والبيانات.
- ☒ نوع من أنواع الاحتيال عبر الإنترنت، حينما يتم تهديد الضحية بتدمير البيانات أو دفع فدية.
- ☒ ويتم من خلال شراء بيانات بطاقات الائتمان واستخدامها لشراء المنتجات عبر الإنترنت.
- ☒ يعتمد على خداع الآخرين عبر برامج تغيير الصوت لإقناع الضحايا بمشاركة البيانات والمعلومات الشخصية.
- ☒ يتم فيه إيهام البائع بأن المشتري قام بالدفع وبعد إرسال المنتج لا تُضاف الأموال إلى رصيده.
- ☒ يستخدم مجرمو الاحتيال الإلكتروني أسماء جمعيات خيرية وهمية من أجل الحصول على الأموال عن طريق إثارة تعاطف الآخرين.
- ☒ يتم أثناء تسوق الضحية، وبعد دفع قيمة المنتج لا يصل إليه أي شيء، أو ربما يصل إليه منتج خاطئ أو مُقلد.

التمرين الثالث

املأ الفراغات بالكلمات المناسبة:

يَعَدُّ 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 **الأموال** ويمكن أن يتم استغلال الهوية في فتح **حسابات** بنكية، أو الحصول على بطاقات **ائتمان** أو قروض، أو من أجل تسجيل خطوط **هاتفية**

يمكن لمُجرمي الاحتيال عبر الإنترنت سرقة **البيانات** الشخصية للاستيلاء على **الحسابات** البنكية المفتوحة بالفعل للشخص، عن طريق **بيانات** شخصيته.

لا بُدَّ أن تتجنب إعطاء الآخرين أيّ **بيانات** شخصية، كما يجب أن تحذف أيّ مستند أو ملف يحتوي على **معلومات** سرّية أو أرقام بطاقات **ائتمان** قبل التخلص منه.

1

2

3

4

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

عليك أن تنتبه جيدًا في تعاملاتك مع **المواقع** التجاريّة، أو مع الآخرين، سواءً من خلال الهاتف أو **البطاقات الائتمانيّة** أو الإنترنت بشكلٍ عامّ، خاصّةً منصات **التواصل الاجتماعيّ**

تجنّب فتح أيّ **مواقع** غير موثوقة، وقم بإلغاء **النوافذ** المنبثقة، وتأكد من **بيانات** الشخص الذي تتحدّث إليه عبر الإنترنت.

استخدم **كلمة سرّ** قويّة على هاتفك وحساباتك الشخصيّة، ولا تشاركها مع الآخرين، ولا تنس الاحتفاظ **بنسخة** احتياطية لبياناتك، وتجنّب استخدام شبكات **Wi-Fi** العامّة، خاصّةً إذا كنت ستفتح أيّ تطبيق له علاقة بمعاملاتك البنكيّة.

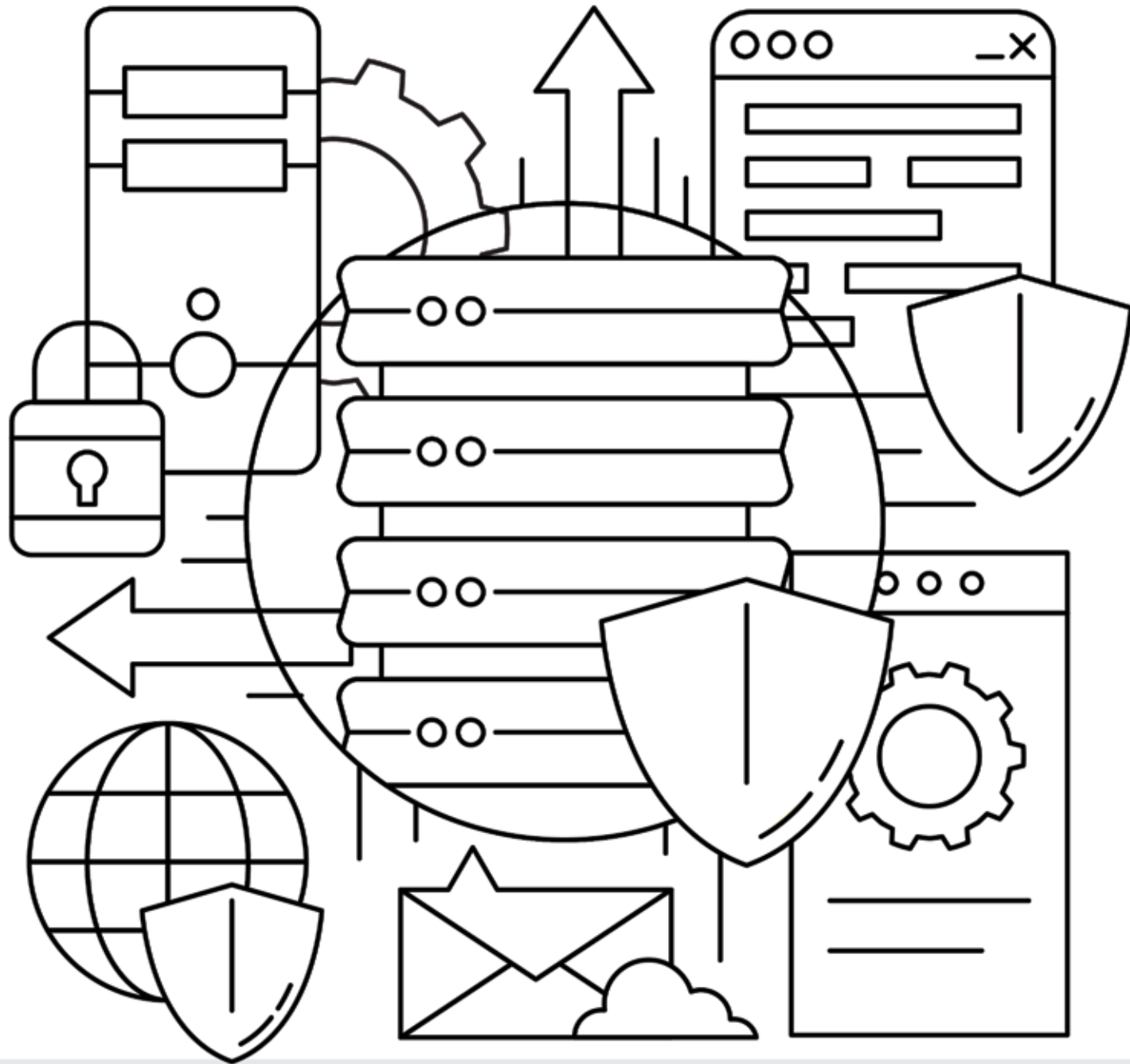
إذا كنت ترغب في التسوّق **عبر الإنترنت** فعليك أن تتأكد من الثّقة بهذا المتجر، وأن تقرأ تقييمات الآخرين ومراجعاتهم، ومن الأفضل التّعامل مع المتاجر المشهورة والتي تُعرّف بالأمان.

انْتَبِه!

الاحتيال المعلوماتي

الخداع أو الغش المعلوماتي الذي يقوم على التلاعب في نظم المعالجة الآلية للمعلومات، بفرض الحصول دون وجه حق على خدمات أو أموال أو أصول معينة.





التمرين الرابع

ضع علامة (✓) أو علامة (X) أمام العبارات التي
تُعَدُّ أساسيّة للحماية من جرائم الاحتيال الإلكتروني:

✓	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 المعدلة أو المخترقة من التطبيقات الخاصة بالهواتف الذكية.	10

انتبه!

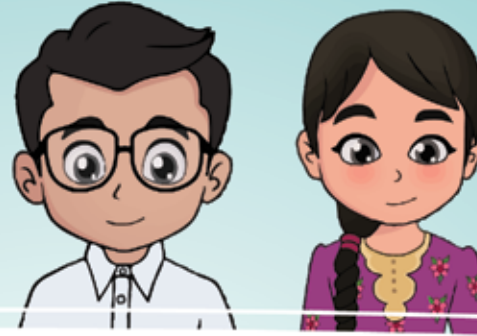
أسباب الوقوع ضحيةً للاحتيال عبر الإنترنت

- 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 المستهدفة عبر الإنترنت.



التمرين الخامس

ضع الكلمة المناسبة
أمام كل جملة:



البصمة الرقمية	1. الأثر الذي تتركه خلفك والمعلومات التي تخلفها بعد كل استخدام للإنترنت.
الاختيال عبر الإنترنت	2. النصب وسرقة البيانات باستخدام تقنيات التكنولوجيا والإنترنت.
برامج مكافحة الفيروسات	3. برامج تساعدك على حماية أجهزتك وصد هجمات المحتالين.
كلمة المرور	4. مجموعة من الحروف والرموز والأرقام التي تستخدم لحماية حساباتك.
تبييض أموال	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.







انتبه!

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

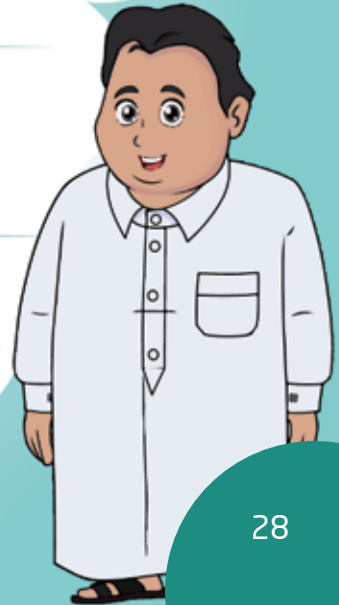
استخرج الكلمات
الثَّالية من الجدول:

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

الاحتِيال - النُّصب - التَّلَاعِب - بَيانات - التَّعليمات - الأوامر - التَّقْيِيَة - الضَّرر
جَريمة - مُجرِم - خِداء - غِش - إفلاس - حَق - عمل

حدّد الصّحيح والخطأ في العبارات التّالية:

- | | | |
|------|---|---|
| صحيح | 1 | يَسْتَفِلُّ مُجْرِمُو الاحتيال عبر الإنترنت ثقة النَّاس من أجل سرقة أموالهم وبياناتهم. |
| صحيح | 2 | يَذَرُسُ الْمُجْرِمُ الإلكترونيّ الضَّحِيَّةَ لمعرفة نقاط ضعفها؛ لكسب الثَّقة قبل القيام بجريمته. |
| خطأ | 3 | الشَّرَكَاتُ الكبرى لا تتعرَّض أبداً لأيّ من جرائم الاحتيال عبر الإنترنت. |
| خطأ | 4 | لا يمكن لجرائم الاحتيال عبر الإنترنت أن تدخل في أيّ مجالات أخرى غير سرقة الأموال والبيانات. |
| خطأ | 5 | لا يسعى مُجْرِمُو الاحتيال عبر الإنترنت إلّا إلى الحصول على الأموال فقط. |



6 استخدام التطبيقات غير القانونية يُساعد مرتكبي جرائم الاحتيال عبر الإنترنت. **صحيح**

7 يمكن تحميل التطبيقات من أيّ موقع على الإنترنت دون خوف. **خطأ**

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

9 لا تحتاج إلى استخدام برامج مكافحة الفيروسات. **خطأ**

10 استخدِم الأرقام من 1 إلى 8 كلمة مرور لحساباتك وأجهزتك. **خطأ**



خطأ

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

11

خطأ

لا يمكن الاحتيال باسم المؤسسات الخيرية أو التطوعية.

12

صحيح

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

13

صحيح

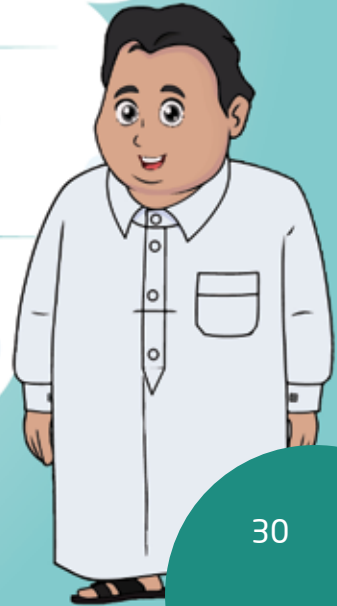
الروابط الخبيثة التي تُضَفَّط عليها دون وعي قد تتسبب في سرقة بياناتك وحساباتك.

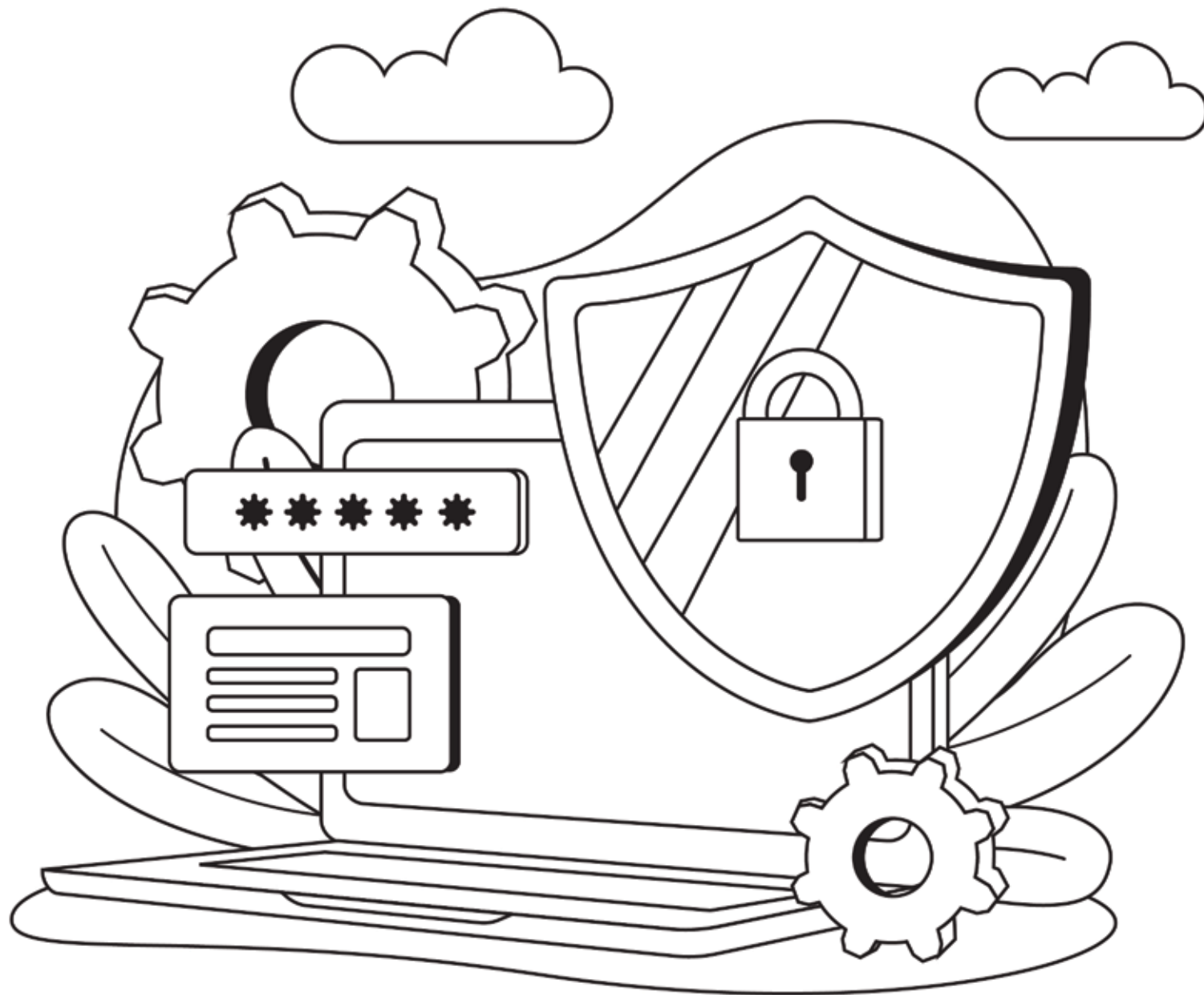
14

خطأ

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

15





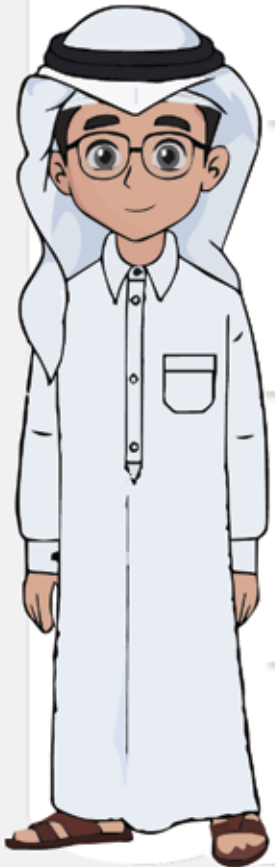
التمرين الثالث

أكمل الجمل التالية:

1... **البصمة الرقمية**... هي الظل الرقمي، وتعني أثر البيانات التي تتركها عند استخدام الإنترنت.

2 تشمل البصمة الإلكترونية زيارات **المواقع الإلكترونية**، ورسائل **غرف الدردشة**، والمعلومات التي تبحث عنها.

3 البصمة الرقمية... **النشطة**... وهي حين تشارك معلومات عن نفسك عن عمدٍ من خلال المشاركة في مواقع **الإنترنت**... أو المنتديات.



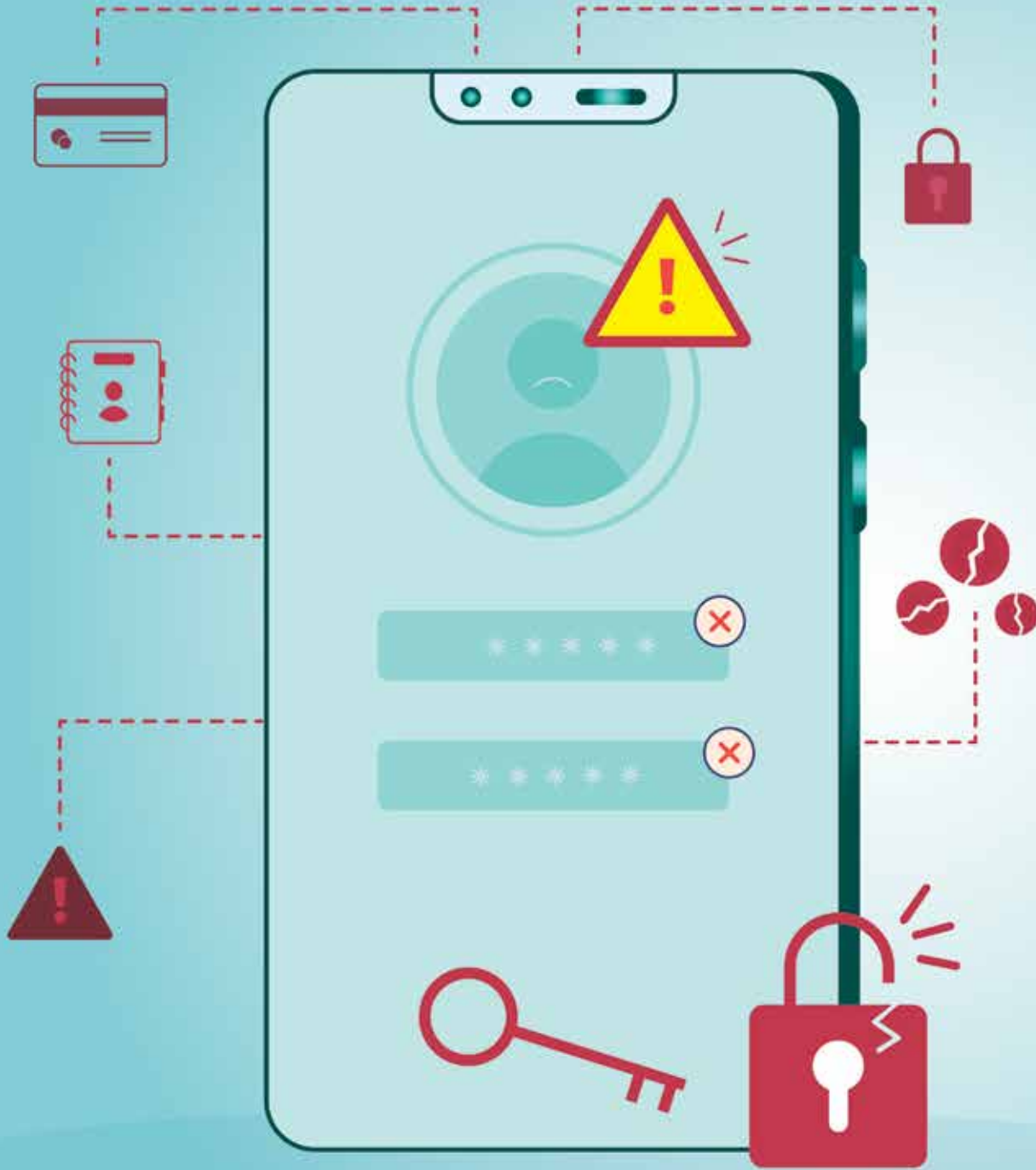


البصمة الرقمية **غير النشطة** تحدث من خلال جمع المعلومات حول المستخدم دون أن يدرك ذلك، سواء من زيارته للمواقع أو المعلومات التي يبحث عنها ويستخدم فيها عنوان الـ **IP** الخاص به.

4

للبصمة الرقمية أهمية كبيرة؛ خاصة أنها تُقدِّد بيانات **شخصية** وتُحدِّد السَّمعة **الرقمية** للشخص، وتلجأ بعض جهات العمل إلى تتبُّع **البصمة** الرقمية الخاصة بالموظفين المُحتملين، ويمكن أن يُساء تفسير بعض الكلمات أو **الصُّور** التي تشاركها على الإنترنت؛ ممَّا يُؤثِّر على سَمعتك أو **بصمتك** الرقمية.

5



هل تعلم؟

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



التمرين الرابع

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

✓	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. احذر 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 كل 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.

في حال ذكر الطالب معلومات حول أنه من الخطأ فتح الروابط الغريبة، إضافةً لذكره معلومات حول عدم التّعامل مع الرّسائل المجهولة التي تتضمّن جوائز أو هدايا، فهذه الرّسائل تُعدّ مقدّمة لعملية احتيال إلكترونيّ.

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.

في حال ذكر الطالب معلومات حول أنه من الخطأ تقديم معلومات شخصية لأيّ جهة على الإنترنت، أو تقديم معلومات حول كلمات المرور.

في حال ذكر الطالب أنه من الخطأ تصديق أيّ جهة على الإنترنت تدّعي أنها جهة رسمية وتطلب معلومات شخصية أو كلمات مرور.



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

في حال ذكر الطالب معلومات حول عدم صحة إعطاء أي معلومات شخصية أو معلومات تخص الحسابات المالية لأي شخص أو جهة تتصل وتدعي أنها تحمل صفة رسمية، فالبنوك لا تطلب معلومات من العملاء عن طريق الاتصال.

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.

في حال ذكر الطالب أن انتحال صفة جمعيات خيرية أو منظمات إنسانية يعد

من أدوات الاحتيال الإلكتروني، وأنه لا يجوز التعامل مع هكذا منظمات أو

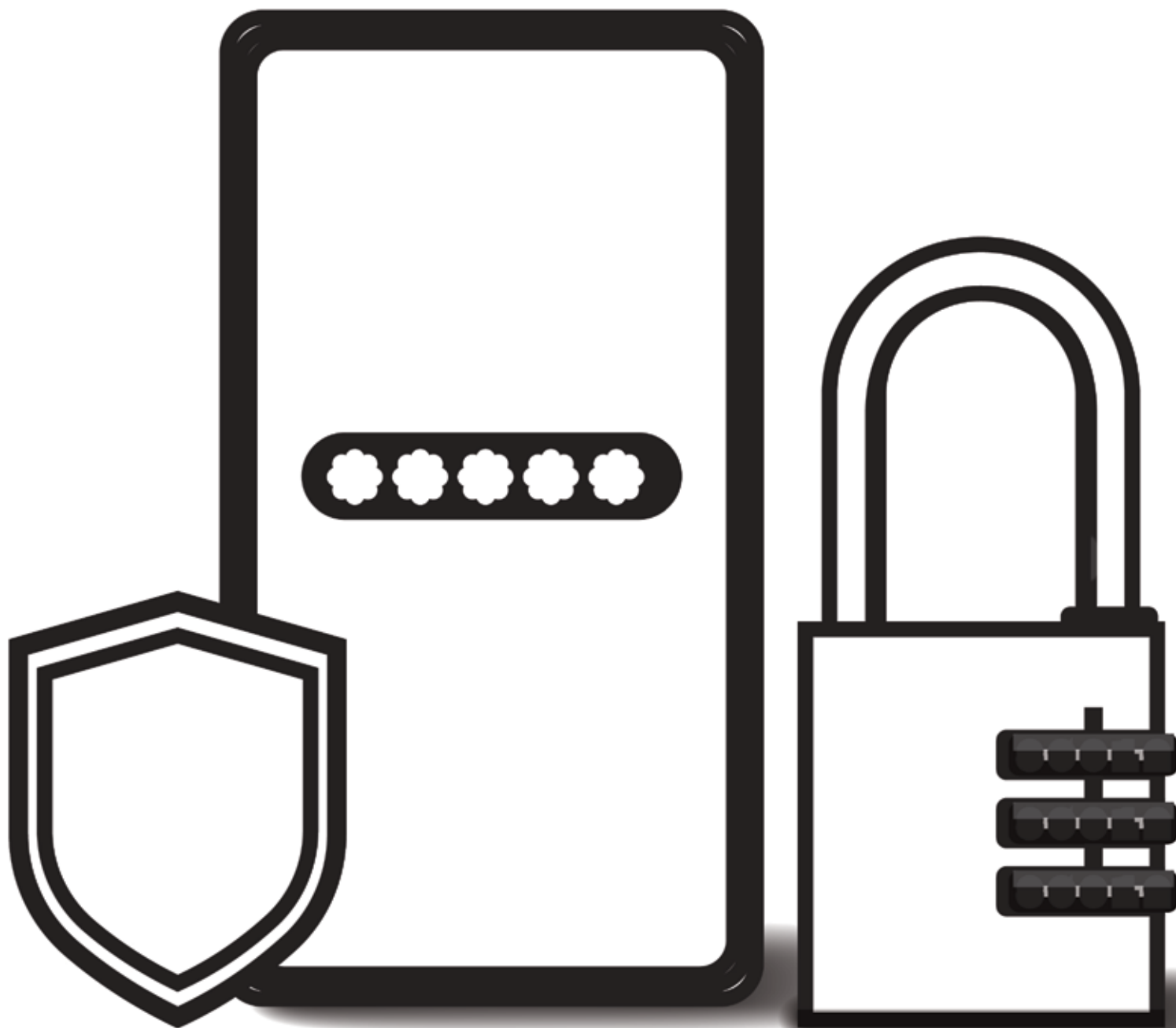
جمعيات إلا من خلال المواقع الرسمية ومن خلال إيصال رسمي يثبت قيمة التبرع.



هل تعلم؟

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





تَتَكَوَّنُ البَصْمَةُ الرَّقْمِيَّةُ مِنْ خِلالِ

1 التَّسَوُّقُ عِبرَ الْإِنْتَرْنِتِ.

2 التَّسْجِيلُ لِإِنْشَاءِ حِسَابٍ عَلَى مَوْقِعٍ وَبِئِيبٍ مَعْيِنٍ.

3 تَنْزِيلُ التَّطْبِيقَاتِ وَاسْتِخْدَامُهَا.

4 اسْتِخْدَامُ وَسَائِلِ التَّوَاصُلِ الْاجْتِمَاعِيِّ عَلَى الْأَجْهَظَةِ الْخَاصَّةِ بِكَ.

5 تَسْجِيلُ الدُّخُولِ إِلَى مَوَاقِعِ الْوَيْبِ الْآخَرَى بِاسْتِخْدَامِ بَيَانَاتِ Facebook.

6 التَّوَاصُلُ مَعَ الْأَصْدِقَاءِ وَجِهَاتِ الْإِتِّصَالِ عِبرَ الْإِنْتَرْنِتِ.

7 مِشَارَكَةُ الْمَعْلُومَاتِ وَالبَيَانَاتِ وَالصُّوَرِ مَعَ مَعَارِفِكَ.

طرق حماية البصمة الرقمية

1 التَّحَقُّق من المعلومات الخاصَّة بنا عبر استخدام محرِّكات البحث.

2 إزالة المعلومات الشَّخصيَّة من المواقع الإلكترونيَّة.

3 تقييد كمِّيَّة البيانات التي يتمَّ مشاركتها عبر الإنترنت.

4 التَّحَقُّق من إعدادات الخصوصية بمواقع التَّواصل الاجتماعيِّ.

5 تجنُّب المواقع غير الآمنة.

6 الحَذَر عند استخدام شبكة Wi-Fi عامَّة.

7 حذُف 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 التَّحرُّك 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 التّسوّق 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 اللّوحية.

☒ صحيح.

☐ خطأ.

6. من أسباب الاحتيال عبر الإنترنت:

☐ عدم اتباع قواعد التّصفح الآمن للإنترنت.

☐ التّعامل مع المتاجر الإلكترونيّة غير الموثوقة.

☐ استغلال مشاعر التّعاطف.

☒ 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.

☐ تسرّب البيانات.

☒ جميع ما سبق.

12. يمكن استخدام لتتبع أنشطة أي شخص عبر الإنترنت.

☐ بصمة الوجه.

☐ بصمة اليد.

☒ البصمة الرقمية.



صل 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)

- ☐ استغلال حالات الطوارئ مثل جائحة كورونا.
- ☐ أحد أشكال الاحتيال عبر الإنترنت.
- ☐ سرقة العملات الرقمية خلال السنوات الأخيرة مثل البيتكوين.
- ☐ اليوم الصفر Zero-day.
- ☐ أمان المعلومات.
- ☐ سرقة البيانات.
- ☐ انتهاك البيانات.

ضع الكلمة أو العبرة المرادفة للجمل التالية

هجوم الفدية

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

الاختيال عبر الإنترنت

رسائل بجوائز مالية وهدايا مُزيّفة تصل إلينا عبر البريد الإلكتروني أو Messenger، وهَدَفُها خداعنا وسرقة بياناتنا.

الثغرات الأمنية

نقاط ضعف تتسبّب في خرق أجهزتنا، سواء الحاسوب أو الهاتف الذكي أو الأجهزة اللوحية، وتُعرّضنا للخطر.

أمان المعلومات

أدوات تحمي معلوماتنا الحساسة من الوصول إليها وتعطيها أو إتلافها.

انتهاك البيانات

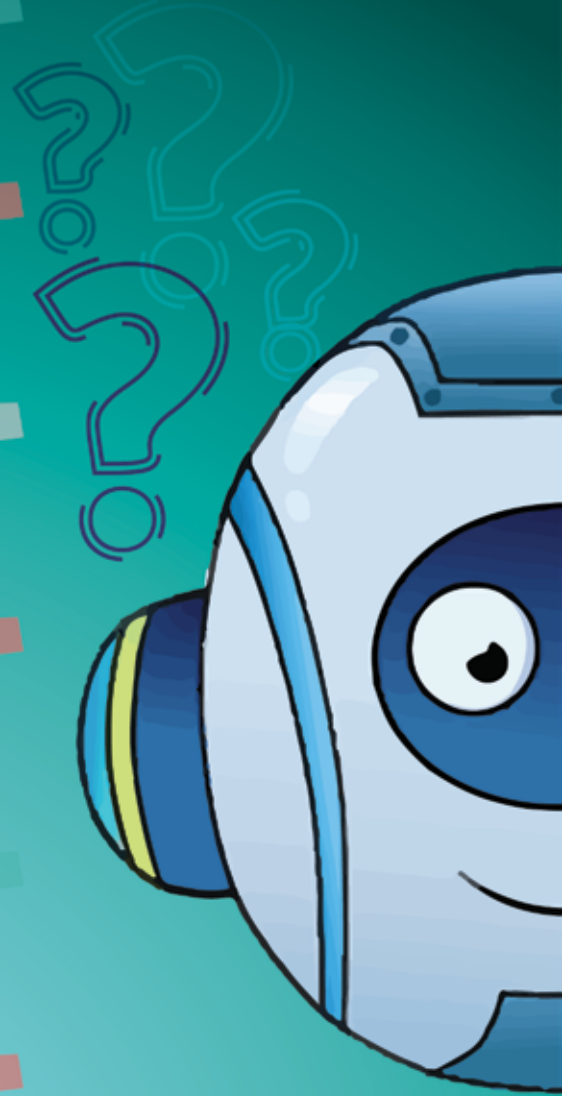
سرقة من نوع خاص تستهدف بياناتنا الشخصية على الإنترنت ويعاقب القانون فاعلها.

البصمة الرقمية

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

كلمة المرور

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





أكمل الجمل التالية بالإجابات الصحيحة:

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

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

3 يستطيع مُجرمو الإنترنت استغلال **البصمة الرقمية**. لأغراض مثل سرقة الهوية عبر الإنترنت.

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

5 من طرق حماية البصمة الرقمية تقييد **كمية البيانات التي يتم مشاركتها** ...



6 التَّحَقُّق من إعدادات الخصوصية من طرق حماية **البصمة الرقمية**...

7 من إرشادات الحماية من الاحتيال عبر الإنترنت تجنُّب الرِّوابط **مجهولة المصدر**...

8 يَفْضَل أن تُستخدَم كلمات مرور مَكُونَة من **الحُرُوف، والرُّموز، والأرقام**... للحماية من الاحتيال عبر الإنترنت.

9 في حال التَّعرُّض لجريمة الاحتيال عبر الإنترنت نلجأ إلى إبلاغ **شخصي ثقة، مثل الوالدين**...

10 إذا كانت شاشتك تمتلئ بشكلي مفاجئ بالتوافذ المنبثقة، فيجب **غلقها على الفور**...

انْتَبِه!

البَصْمَةُ الرَّقْمِيَّة

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

وتُحدد **البصمة الرقمية** سُمُعة الأشخاص على الإنترنت كما يَحْدُث في الحياة العادية.





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



مشروع التَّخْرِجُ

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

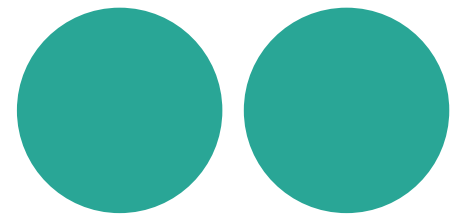


كِتَابَةُ قِصَّةٍ قَصِيرَةٍ تَحْدُورُ أَحْدَاثُهَا حَوْلَ طَالِبٍ تَعَرَّضَ لِمَحَاوَلَةِ إِحْتِيَالٍ عِبْرَ الْإِنْتَرْنِتِ، وَكَيْفَ تَصَرَّفَ جَيَالُ هَذَا الْمَوْقِفِ.



مراجع

المحتوى العلمي
في الحقيقة



المراجع العربية:

1. احم نفسك من عمليات الاحتيال والهجمات عبر الإنترنت، مايكروسوفت. مُتاح على الرابط: <https://cutt.us/YVxY1>
2. أشهر طرق الاحتيال عبر الإنترنت التي انتشرت في السنوات الأخيرة، روسيا اليوم، 2020م. مُتاح على الرابط: <https://cutt.us/gDg5J>
3. حمادي، خالد. البصمة الرقمية... الظل الإلكتروني الخفي، جامعة العربي التبسي تبسة، الجزائر، يوليو 2021م، مُتاح على الرابط: <https://cutt.us/QToSN>
4. القرصنة الإلكترونية: سرقة 600 مليون دولار في عملية احتيال ضخمة بالعمليات الرقمية، بي بي سي عربي، 2021م. مُتاح على الرابط: <https://cutt.us/ToS7P>
5. ما المقصود بسرقة البيانات وكيفية منعها؟، Kaspersky. مُتاح على الرابط: <https://cutt.us/Ve2to>
6. ما هو بأمان المعلومات؟، مايكروسوفت. مُتاح على الرابط: <https://cutt.us/CxorE>
7. يونس الباشا، فائزة. الجريمة المنظمة في ظل الاتفاقيات الدولية

والقوانين الوطنية، دار النهضة العربية للطبع والنشر والتوزيع، 2001م، ص 21.

المراجع الأجنبية:

1. 300m in cryptocurrency' accidentally lost forever due to bug, The Guardian. On site: <https://cutt.us/ILdpQ>
2. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, The New York times. On site: <https://cutt.us/oOhv7>
3. Computer and Internet Fraud, Impact Law. On site: <https://cutt.us/DtS4E>
4. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: <https://cutt.us/ZMXpW>
5. How to Handle Zero-day, Nordic Defender, 2022. On site: <https://cutt.us/gUQ7g>

13. Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: <https://cutt.us/TvLAe>
14. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: <https://cutt.us/ZwCye>
15. What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: <https://cutt.us/teSUS>
16. What was the WannaCry ransomware attack? cloudflare. On site: <https://cutt.us/8jM6q>
17. What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: <https://cutt.us/FXNvU>
18. What is bug? Neterich. On site: <https://netenrich.com/glossary/bug>
19. What is email fraud? Cloudflare. On site: <https://cutt.us/mg8Sf>
20. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: <https://cutt.us/Tr7jj>
6. How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. Onsite: <https://cutt.us/G7awc>
7. How to protect your digital footprint, state farm, 2023. On site: <https://cutt.us/OcHUG>
8. Internet Fraud, Australian Federal Police (AFP). on site: <https://cutt.us/leAYp>
9. Mobile phone fraud, Action Fraud - National Fraud&Cyber Crime Reporting Centre. On site: <https://cutt.us/1FoJG>
10. Ransomware News, Ransomware Timeline: Top Stories December 2017, Cyber defense magazine. On site: <https://cutt.us/IJBEQ>
11. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: <https://cutt.us/fVN5g>
12. Toyota Boshoku Corporation loses \$37 million in Business Email Compromise scam, CYWARE SOCIAL. On site: <https://cutt.us/fFDMv>





CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency