الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

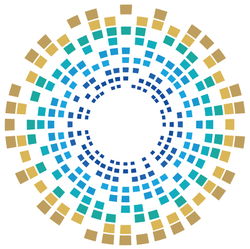
مبادئ عامة في السلامة الرقمية

الشريحة المُستهدَفة: العمالة الوافدة

كُتَيّب المدرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

العمالة الوافدة

كُتَيّب المُدَرّب

تمهيد

السَّلامة الرقميَّة ركيزة أساسيَّة لضمان أمْن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تم تصميم هذا الكُتَيِّب بهدف توعية كبار القَدْر بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيِّب إلى تعزيز وعيهم حول تهديدات سيبرانية، مثل التصيد الاحتيالي، والبرمجيَّات الضَّارَّة، وتمكينهم من حماية بياناتهم وأجهزتهم بشكلٍ فعّالٍ.

وتُعدّ هذه الجهود جزءاً من المبادرة الوطنية للسلامة الرقمية التي تُنظِّمها الوكالة الوطنية للأمن السيبراني، لبناء بيئة رقمية آمِنَة لجميع فئات المجتمع.

تعريف المبادرة

مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

وتعمل على نشر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومتمكّن تكنولوجيًّا.

الشرائح المستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها في السنة الأولى على الشرائح التالية:

- كبار القَدْر
- المرأة والأسرة
- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي

أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

- دليل السلامة الرقمية
- كتيبات توعية
- ألعاب سيبرانية
- فيديوهات توعية
- ألعاب تعليمية مبتكَرة
- ورش توعية

المخاطر السيبرانية الشّائعة

التصيد الاحتيالي

التصيد الاحتيالي هو نوع من الهجمات الإلكترونية التي يستخدم فيها المهاجمون رسائل هاتفية أو رسائل بريد إلكتروني أو مواقع ويب مزيَّفة؛ لخداع الأشخاص للكشف عن معلومات حسَّاسة، مثل كلمات المرور، أو بيانات الحسابات المصرفية.

معلومة

البنوك والمؤسسات المالية لا تَطلب مِن عُملائها تزويدها بأيّ بيانات مُهِمَّة عن طريق الهاتف

مثـــال عمـــلي

إذا فتحت رابطًا مزيفًا يَطلب منك بيانات حسابك البنكي؛ يمكن للمخترق سرقة أموالك أو معلوماتك الشخصية. لذلك، فالتحقُّق مِن روابط المواقع والبريد الإلكتروني قبل إدخال أيّ معلومات أمر ضروري.

مَراحل تنفيذ هجمات التصيد الاحتيالي

الرسائل الاحتيالية

المهاجِم يرسل بريداً إلكترونياً يبدو وكأنه من مصدر موثوق، مثل بنك أو شركة معروفة.

المواقع المزيَّفة

الرسالة تحتوي على رابط يقود إلى موقع مُزيَّف يبدو مشابهاً للموقع الأصلي؛ حيث يُطلَب من الضحية إدخال معلوماته الشخصية.

استغلال المعلومات

بمجرَّد أن يُقدّم الضحية بياناته، يتم استخدامها لسرقة الأموال أو الوصول إلى حساباته الخاصة.

وسائل تنفيذ هجمات التصيد الاحتيالي

رسائل البريد الإلكتروني والرسائل الاحتيالية التي تبدو شرعية.

المكالمات الهاتفية أو رسائل البريد الصوتي الاحتيالية.

النوافذ المُنبثِقة والإعلانات المُضلّلة.

العروض الترويجية الوهمية.

حقائق ومعلومات

تَعتمـد برمجيـات الفديـة علـى تشـفير الملفات الخاصـة بالضحايا، ومُطالبتهم بدَفْـع مبالغ ماليـة مقابل فَكّ التشـفير

سؤال تفاعلي

هل يمكنك تمييز رسالة بريد إلكتروني مشبوهة؟ وما العلامات التي قد تشير إلى أنها محاولة تصيّد؟

سؤال تفاعلي

هل سبق أن استخدمت شبكة Wi-Fi عامة؟ كيف يمكنك حماية حساباتك المالية عند استخدام هذه الشبكات؟

مخاطر التصيد الاحتيالي

1

سرقة البيانات الشخصيَّة

الحصول على معلومات حسَّاسة مثل كلمات المرور وأرقام البطاقات البنكية

2

اختراق الحسابات المالية

الوصول إلى الحسابات البنكية وسرقة الأموال

3

الابتزاز الإلكتروني

استخدام البيانات المسروقة للضَّغط على الضحايا لدفع فدية

4

إصابة الأجهزة ببرمجيات خبيثة

زَرْع برمجيات ضارَّة عند النَّقْر على الرَّوابط المزوّرة

5

انتحال الهُويَّة

استخدام المعلومات المسروقة للقيام بأنشطة غير قانونية باسم الضحية

سرقة البيانات الشخصية

هـي الحصـول غيـر المـصرَّح بـه علـى معلومـاتٍ حسَّاسـة، مثـل أرقـام الهُويَّة، وكلمات المرور، أو بيانات الحسابات البنكية؛ بهدف استخدامها فـي أنشـطة غيـر قانونية.

البرمجيات الضّارّة

برمجيات خبيثة تم تصميمها لإلحاق الضرر بأجهزة الحاسوب أو الشبكات أو سرقة البيانات منها دون عِلْم المُستخدِم. تشمل الفيروسات، وديدان الحاسوب، وبرمجيات التجسُّس، وغيرها.

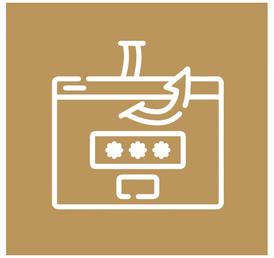
كيف تعمل البرمجيات الضّارَّة؟

1 إصابة النظام

تُزرَع البرمجيات الضّارَّة في النظام عبر تنزيل ملفات مشبوهة أو النقر على روابط غير آمِنَة

2 التنفيذ الخفي

بعد التثبيت، تعمل البرمجيات الخبيثة بصمت دون أن يلاحظ المستخدِم أي تغييرات فَوْرية



3 سرقة المعلومات أو تعطيل النظام

يمكن للبرمجيات الضّارَّة أن تسرق بيانات المُستخدِمين، أو تُعطّل النظام، أو تتسبَّب في خسائر مالية

علامات إصابة الجهاز بالبرمجيات الضّارَّة (Malware)

1

تَراجُع أداء الجهاز

لأن البرمجيات الضّارَّة تستهلك موارد النظام

2

ظهور نوافذ مُنبثِقة غير مرغوب فيها

مثل إعلانات متكررة وتحذيرات مزيَّفة حول وجود تهديدات

3

تغييرات مفاجئة في النظام

مثل تغيير الصفحة الرئيسة للمُتصفّح، وظهور شريط أدوات جديد

4

استهلاك مرتفع للبيانات غير معروف السبب

5

إرسال رسائل بريد إلكتروني بشكلٍ تلقائي

6

ظهور ملفات أو مجلدات جديدة أو اختفاؤها

برمجيات التجسُّس (Spyware)

نـوع مـن البرمجيـات الخبيثـة التـي تجمـع معلومـات عـن المُسـتخدِمين دون علمهـم أو موافقتهـم، وتشـمل:

- **برمجيات تسجيل نقرات المفاتيح (Keyloggers):** تسمح للمهاجمين بسرقة كلمات المرور، والبيانات الشخصية والمالية التي يتم إدخالها عبر لوحة المفاتيح.
- **برمجيـات الإعلانـات (Adware):** برمجيـات تعـرض إعلانـات غيـر مرغـوب فيهـا علـى جهـاز المُسـتخدِم، وتجمـع بيانـات عـن تصفُّـح المُسـتخدِم.
- **تتبُّع ملفات تعريف الارتباط (Tracking Cookies):** ملفات نصية صغيرة تُحفظ على جهاز المُستخدِم لتتبُّع نشاطه على الإنترنت.
- **برمجيات مراقبة النظام (System Monitors):** برمجيات تراقب نشاط النظام وتجمع بيانات عن كيفية استخدام الحاسوب.

لنَحْذَر!

يجب عدم إرسال بيانات حساسة، مثل كلمات المرور أو معلومات الحسابات المصرفية، عبر اتصالات غير مشفَّرة، مع استخدام قنوات آمِنَة دائمًا

برمجيات التجسُّس عن طريق الكاميرا (Spyware on camera)

1. هي برمجيات تجسُّس تقوم بالتشغيل الآلي لكاميرا الهاتف الذكي أو جهاز الحاسوب

2. يقوم البرنامج بنقل الفيديو المسجَّل إلى المهاجم؛ بهدف التجسس على خصوصية الضحية أو ابتزازه مالياً

حقائق ومعلومات

الشركات الصغيرة والمتوسطة عادةً ما تكون أقل استعداداً للتعامل مع الهجمات السيبرانية؛ مما يجعلها هدفاً شائعاً للقراصنة

مخاطر برمجيات التجسُّس (Spyware)

1

سرقة الهوية

تستهدف برمجيات التجسُّس الهوية الرقمية للضحايا، والبيانات الشخصية

2

الابتزاز

من خلال استخدام المعلومات الحسَّاسة المسروقة لابتزاز الضحايا

3

فقدان الخصوصية

تتبُّع النشاط على الإنترنت وجمع البيانات الشخصية دون عِلْم المستخدِم يؤدي إلى انتهاك خصوصيَّته

4

تَراجُع أداء الجهاز

تُؤدّي برمجيات التجسس إلى إبطاء الجهاز بسبب العمليات التي تقوم بها لجمع البيانات

حقائق ومعلومات

الأجهزة المنزلية الذكية التي تعتمد على إنترنت الأشياء يمكن أن تكون عرضة للاختراق إذا لم يتم تأمينها بشكلٍ صحيحٍ

آليات الوقاية والسلامة الرقمية

كيفية التعرُّف على رسائل البريد الإلكتروني والرسائل الاحتيالية

1. عدم مطابقة البريد الإلكتروني أو الهاتف الخاص بالمُرسل مع اسم المؤسسة المعروفة.
2. اختلاف البريد الإلكتروني أو الهاتف المُستخدَم عن المُعلَن من المؤسسة التي يستغل اسمها في تنفيذ الهجوم الاحتيالي
3. الرَّابط في الرسالة قد يبدو صحيحاً، لكنَّه لا يُطابِق الموقع الرَّسمي للمؤسسة
4. اختلاف الرسالة بشكلٍ واضحٍ عن الرسائل الأخرى التي سبق تَلقّيها من المؤسسة
5. تطلب الرسالة معلومات شخصية مهمة، مثل: رقم بطاقة الائتمان، أو كلمة مرور الحساب
6. الرسائل تكون غير مرغوب فيها وتتضمَّن مُرفَقات غير متوقَّعة

لنَحْذَر!

رسائل البريد الإلكتروني التي تطلب منك بيانات شخصية أو مالية، قد تكون جزءًا من محاولات تصيُّد احتيالي لسرقة هويَّتك

الحماية من التصيد الاحتيالي

- عدم تقديم أيّ معلومات لأيّ شخص قبل التأكد التّامّ من هُويّته.
- تثبيت برامج مكافحة الفيروسات وتحديثها باستمرار.
- عمل نُسْخة احتياطية من البيانات على مُحرّك أقراص ثابت خارجي أو في السحابة.
- تفعيل المصادقة الثنائية (2FA) للحسابات الشخصية والمالية.

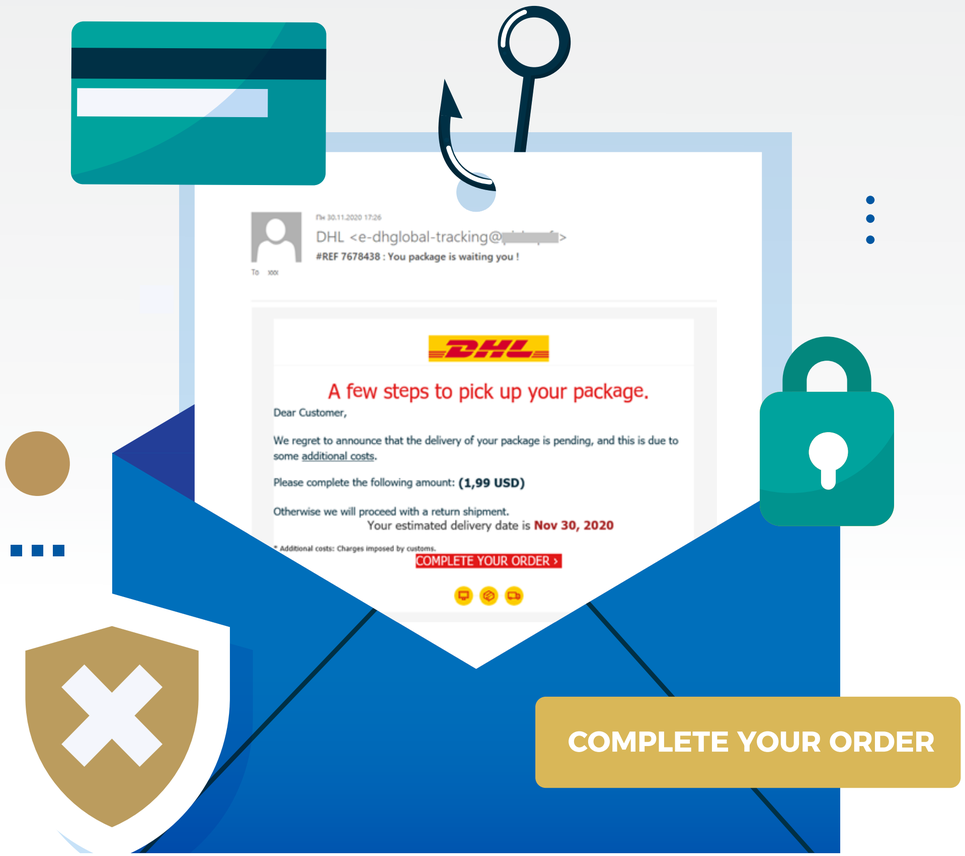
طُرق تجنُّب هجمات التصيد الاحتيالي

1. تعزيز الوعي السيبراني والإلمام بأكثر التحديات الرقمية شيوعًا
2. التفكير جيّداً قبل الضغط على الروابط في رسائل البريد الإلكتروني والرسائل الفَوْرية العشوائية
3. تأكَّد من أمان الموقع عبر التحقُّق من أن عنوانه يبدأ بـ https، ووجود رمز قفل مُغلَق بجانب شريط العناوين
4. التحقُّق من الحسابات عبر الإنترنت بانتظام، وتغيير كلمات المرور بشكلٍ مستمر
5. التحقُّق من البيانات المالية بانتظام، ومراجعة الكشوفات الشهرية للحسابات بدقَّة
6. تحديث المُتصفّح باستمرار؛ للاستفادة من تصحيحات الأمان للمُتصفّحات الشائعة طوال الوقت.

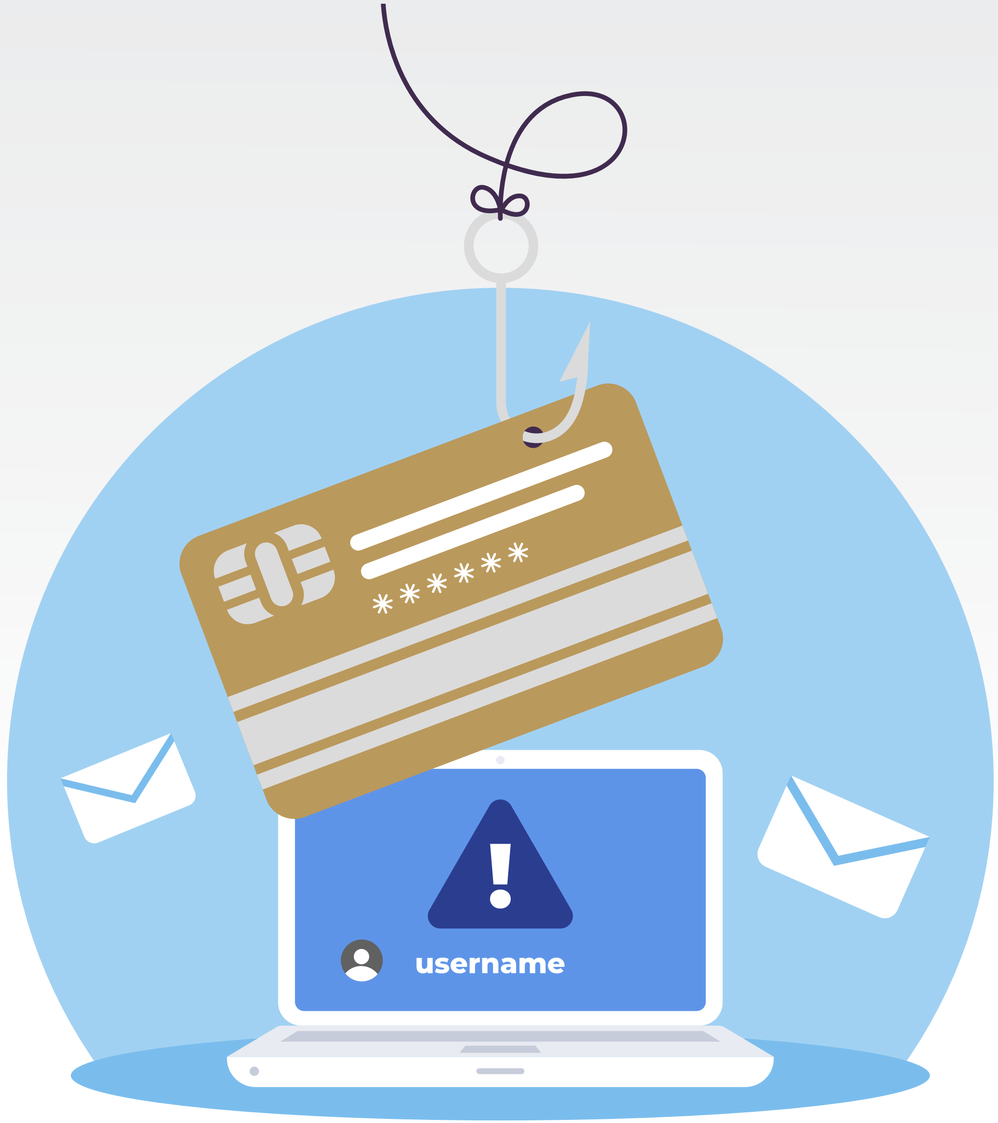
لنَحْذَر!

تجنُّب تثبيت برامج من مواقع غير موثوقة؛ فالبرامج غير المرخَّصة قد تكون مُصابة ببرمجيات خبيثة

نصائح عملية للوقاية من التصيّد الاحتيالي



- تَجاهُل الرَّسائل المشبوهة التي تَطلب معلومات حسَّاسة
- التحقُّق دائمًا من هُويَّة المُرسِل قبل التفاعُل مع الرسالة
- استخدام برامج مكافحة الفيروسات والبريد الإلكتروني المُزوّد بمُرشِّحات التصيد الاحتيالي
- التحقُّق من عنوان URL للمواقع، وتجنُّب الدخول إليها إذا كانت غير موثوقة



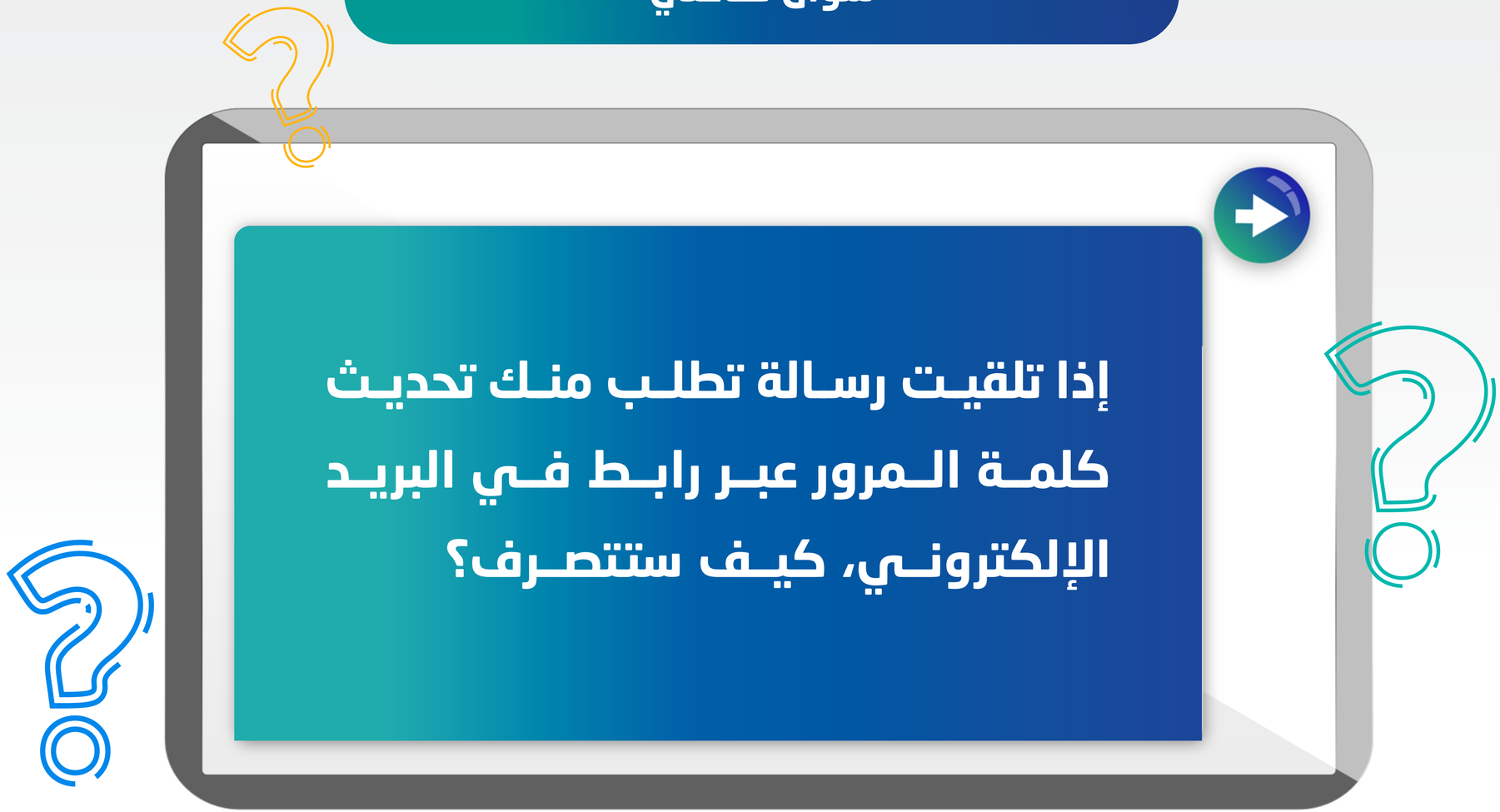
حقائق ومعلومات

استخدام كلمات مرور ضعيفة يُسهّل على المهاجمين اختراق الحسابات بسهولة؛ مما يجعل كلمات المرور القوية ضرورة قُصوَى

سؤال تفاعلي

كيف يمكن التحقُّق من أن الموقع الإلكتروني لمصرفٍ أو مؤسسةٍ ما هو الموقع الرسمي قبل إدخال البيانات الشخصية؟

سؤال تفاعلي


إذا تلقيت رسالة تطلب منك تحديث
كلمة المرور عبر رابط في البريد
الإلكتروني، كيف ستتصرف؟

كيفية التَّصرُّف في حال إصابة الجهاز بالبرمجيات الضّارَّة (Malware)

1. فصل الجهاز عن الإنترنت
2. استخدام وضع الأمان (Safe Mode)
3. استخدام أدوات إزالة البرمجيات الضّارَّة
4. تحديث نظام التشغيل والبرامج
5. استعادة النظام
6. مراجعة أمان الحسابات وتغيير كلمات المرور فورًا

احذر!

تجنَّب استخدام كلمة المرور نفسها لجميع حساباتك على الإنترنت، فإنْ تمَّ اختراق حساب واحد، ستكون بقية الحسابات مُعرَّضة للخطر.

إجراءات الوقاية من سرقة البيانات الشخصية

تجنُّب مشاركة البيانات الشخصية

عبر البريد الإلكتروني أو الرسائل غير الموثوقة

استخدام أدوات حماية الأجهزة

مثل: برامج مكافحة الفيروسات وجدران الحماية

تحديث نظام التشغيل والتطبيقات بانتظام

لضمان سدّ الثغرات الأمنية

إجراءات الوقاية من سرقة البيانات الشخصية

تجنُّب الروابط والملفات المشبوهة:

عدم النقر على الروابط المشبوهة أو تحميل ملفات غير موثوقة

استخدام كلمات مرور قوية:

كلمات مرور مُعقَّدة وغير متوقَّعة

تفعيل المصادقة الثنائية:

إضافة طبقة حماية إضافية

كلمات المرور

- مجموعة من الحروف والأرقام والرموز، يتم إنشاؤها واستخدامها لتأكيد هوية المستخدِم عند محاولة الوصول إلى الأنظمة أو التطبيقات أو البيانات.

- إحدى أهم وسائل المصادقة التي تُساهم في حماية الحسابات والمعلومات من الوصول غير المُصرَّح به.

أهمية كلمة المرور

1

حمـــــــايـــــة الهـــوية الرقمـــية:

تمنع الوصول غير المُصرَّح به إلى الحسابات

2

ســـــــريـــــة البـــــيانـــات:

تَضْمن خصوصية الملفات والمعلومات

3

حمايــة الحسابات الشخصية والمالية:

الخطّ الدفاعي الأول لحماية الحسابات

توصيات لكلمة مرور قوية

01
استخدام كلمات لا تقلّ عن 12 إلى 16 حرفًا

02
المزج بين الحروف الكبيرة والصغيرة، وإضافة أرقام ورموز

03
تجنُّب استخدام الاسم أو تاريخ الميلاد، أو أرقام الهواتف

04
استخدام كلمات فريدة، وعدم تكرارها للدخول إلى حسابات متعددة

05
استخدام كلمة مرور مخصَّصة لكل حساب

06
تجنُّب الأنماط الشائعة مثل: 123456 أو password

07
تغيير كلمات المرور بانتظام (كل 3-6 أشهر)

08
تفعيل خاصية التحقُّق بخطوتين لمزيدٍ من الأمان

التحقُّق ثنائي العوامل (2FA)

آلية أمان إضافية تَستخدم طريقتين مستقلتين لتأكيد هُوية المستخِدم.

مثـــال

إضافة طبقة حماية ثانية بجانب كلمة المرور.

حقائق ومعلومات

المصادقة الثنائية هي إحدى الوسائل الأكثر فعالية لحماية الحسابات الشخصية من الاختراقات السيبرانية

كيفية عمل التحقُّق ثنائي العوامل 2FA

01 إدخال كلمة المرور

02 تقديم دليل إضافي للتحقق، مثل:

- رموز يتم إرسالها عبر الرسائل النصية
- تطبيقات المصادقة
- البصمة أو التعرُّف على الوجه
- مفاتيح أمان مادية

الخطوات التي يجب اتّباعها عند التعرُّض لسرقة البيانات

إبلاغ الجهات المختصَّة

إبلاغ الجهات المسؤولة عن مكافحة الجرائم الإلكترونية

تغيير كلمات المرور فوراً

تغيير جميع كلمات المرور للحسابات المتأثّرة

متابعة الحسابات المالية

مراقبة الحسابات المصرفية وبطاقات الائتمان؛ للكشف عن أي نشاط مشبوه

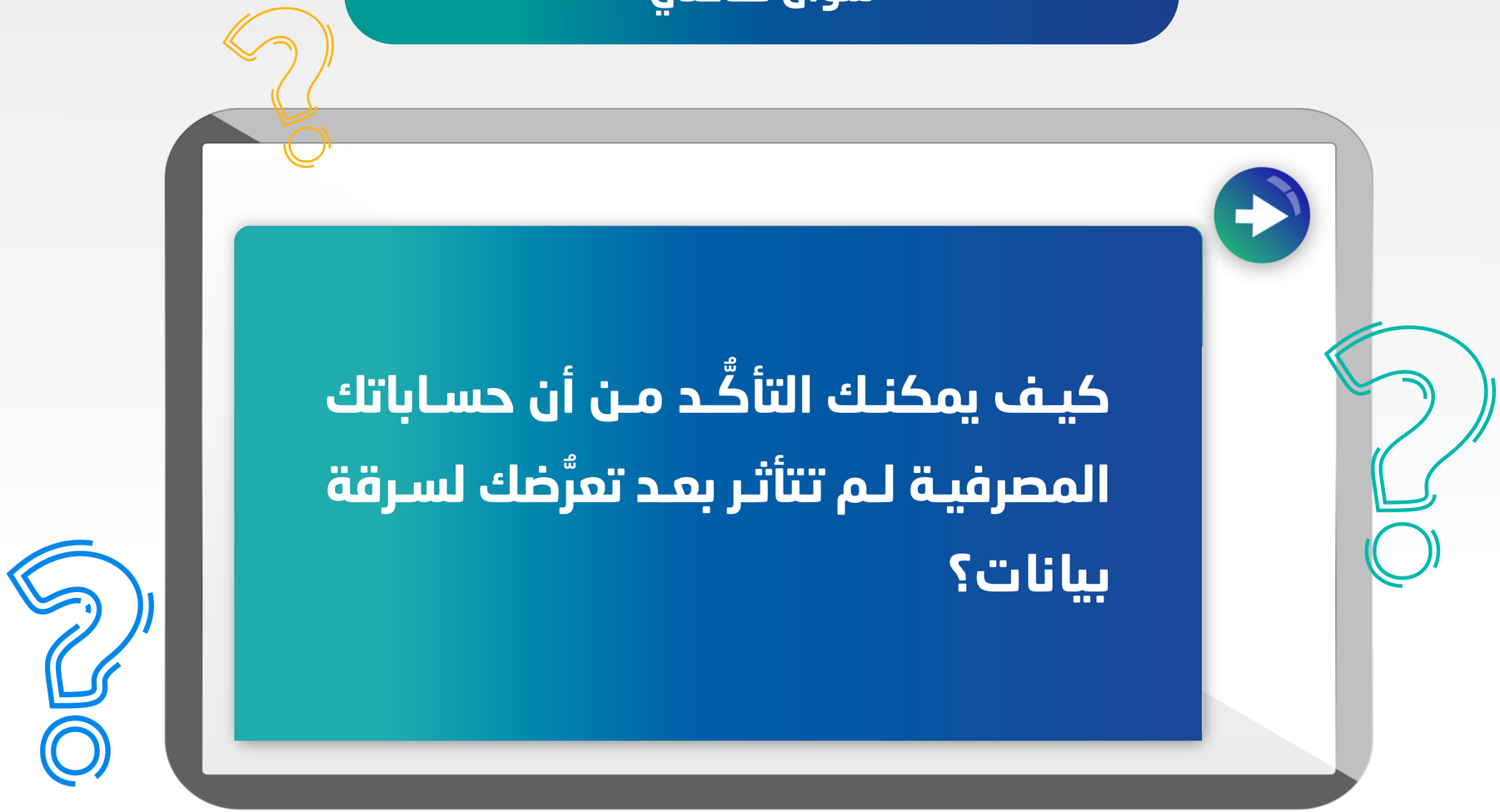
مراجعة الحسابات الرقمية الأخرى

للتأكُّد من عدم استخدام بياناتك في أماكن أخرى

سؤال تفاعلي

إذا علمت أن بياناتك الشخصية قد تمّت سرقتها، ما هي أول خطوة يجب أن تقوم بها؟

سؤال تفاعلي


كيف يمكنك التأكُّد من أن حساباتك المصرفية لم تتأثر بعد تعرُّضك لسرقة بيانات؟

الحماية من البرمجيات الضَّارَّة

1. تحديث نظام التشغيل والبرامج بانتظام
2. تثبيت برامج موثوقة لمكافحة الفيروسات والبرمجيات الضارَّة
3. عدم تحميل برامج أو ملفات من مصادر غير موثوقة
4. ضَبْط إعدادات الخصوصية على الكاميرا والميكروفون
5. تجنُّب استخدام الأجهزة المشتركة أو غير المأمونة للوصول إلى الحسابات الحساسة

الحماية من برمجيات التجسُّس عن طريق الكاميرا

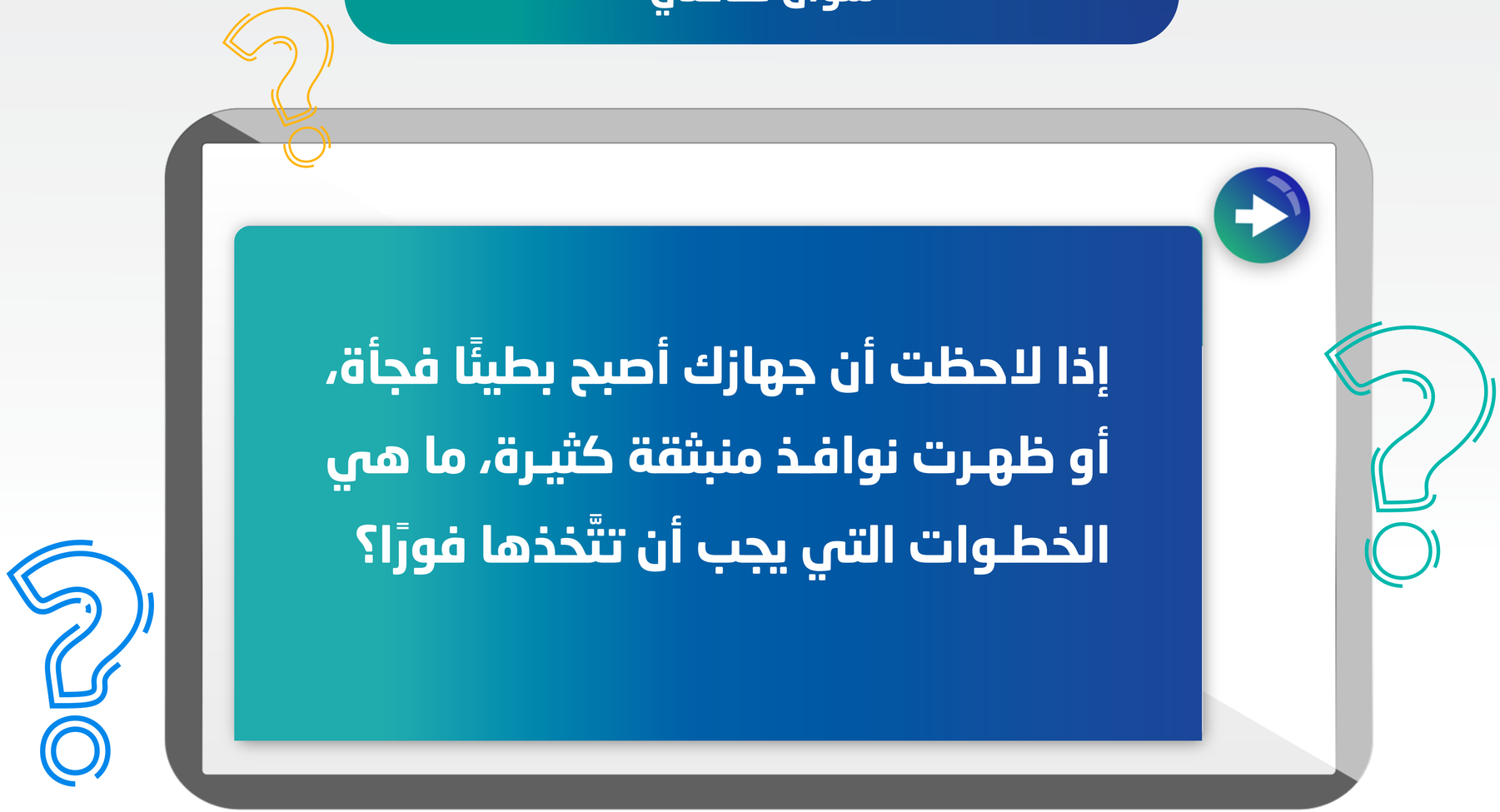
في حالة عمل الكاميرا بشكلٍ تلقائي، توقَّفْ عن استخدام الهاتف الذكي، واطلبْ استشارة متخصّص.

عدم تحميل أو فتح أيّ روابط مجهولة عند إجراء المحادثات.

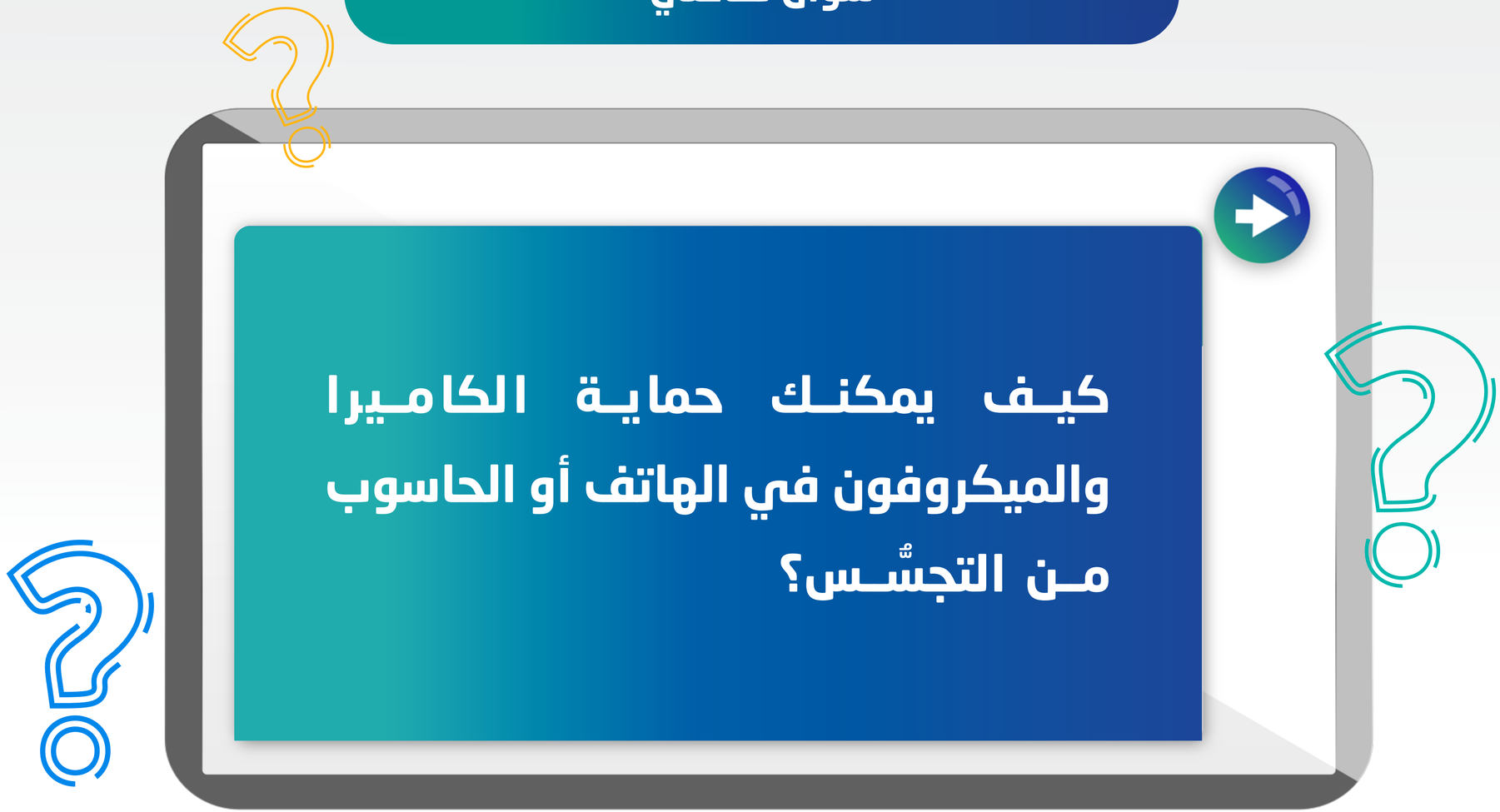
التأكُّد اليدوي من أن الكاميرا في وَضْع الإيقاف.

الفَحْص الدوري للجهاز وتطبيقات الكاميرا؛ بحثًا عن برمجيات ضارة.

سؤال تفاعلي


إذا لاحظت أن جهازك أصبح بطيئًا فجأة،
أو ظهرت نوافذ منبثقة كثيرة، ما هي
الخطوات التي يجب أن تتَّخذها فورًا؟

سؤال تفاعلي


كيـف يمكنـك حمايـة الكامـيرا
والميكروفون في الهاتف أو الحاسوب
مـن التجسّـس؟

ضمان السَّلامة السيبرانية

ما يجب فِعْله	ما يجب تجنُّبه
استخدام كلمات مرور قوية ومعقَّدة.	استخدام كلمات مرور بسيطة وسهلة التخمين.
تفعيل المصادَقة الثنائية للحسابات.	تجاهل إعدادات الأمان الإضافية عند تسجيل الدخول.
تحديث أنظمة التشغيل والبرامج بانتظام.	تأجيل التحديثات الضرورية أو تجاهلها.
التحقُّق من صحة الروابط قبل النقر عليها.	النقر على الروابط الواردة من مصادر غير معروفة.
مراجعة الحسابات البنكية والمالية بشكلٍ دوريّ.	إهمال التحقُّق من الكشوفات المالية.
تنزيل التطبيقات من مصادر موثوقة فقط.	تحميل برامج أو تطبيقات من مواقع غير موثوقة.
الحذر من الرسائل التي تطلب معلومات شخصية.	مُشاركة المعلومات الشخصيَّة عبر البريد الإلكتروني أو الرسائل.
تثبيت برامج مُكافَحة الفيروسات وفَحْص الأجهزة بانتظام.	العمل دون حماية سيبرانية فعَّالة.

خاتمة

تُعدّ السلامة الرقمية مسؤولية شخصية وجماعية تتطلّب الوعي واليقظة، ومن خلال اتّباع نصائح بسيطة مثل استخدام كلمات مرور قوية، وتفعيل المصادقة الثنائية، وتجنّب الروابط المشبوهة، وتحديث الأجهزة والبرامج باستمرار؛ يمكننا تعزيز حمايتنا من التهديدات السيبرانية.

تذكّر أهمية مراجعة الحسابات والبيانات المالية بانتظام، وتجنّب مشاركة المعلومات الشخصية عبر قنوات غير آمِنَة.

عن طريق الوَعْي والالتزام بهذه الإجراءات المُهمَّة؛ نستطيع جميعاً المُشارَكة في بناء بيئة رقميَّة آمِنَة، وتعزيز الأمن السيبراني والسلامة الرقمية في المجتمع.

المراجع

1. الموقع الرسمي للوكالة الوطنية للأمن السيبراني – دولة قطر، المبادرة الوطنية للسلامة الرقمية للعمالة الوافدة، متوفر على الرابط التالي:
https://www.ncsa.gov.qa/initiatives/digital-safety

2. الموقع الرسمي للوكالة الوطنية للأمن السيبراني – دولة قطر، دليل المستخدِم للسلامة الرقمية، متوفر على الرابط التالي:
https://www.ncsa.gov.qa/resources/cybersecurity-guidelines

3. الموقع الرسمي للوكالة الوطنية للأمن السيبراني – دولة قطر، التوعية السيبرانية في بيئة العمل، متوفر على الرابط التالي:
https://www.ncsa.gov.qa/awareness

4. الموقع الرسمي لوزارة العمل – دولة قطر، توجيهات للعمالة الوافدة حول استخدام التكنولوجيا وحماية البيانات الشخصية، متوفر على الرابط التالي:
https://www.mol.gov.qa/en/WorkersDigitalSafety

5. CSO Online. (2023). The Equifax data breach: What happened, who was affected, what was the cost. Retrieved from
https://www.csoonline.com/article/567803/the-equifax-data-breach-what-happened-who-was-affected-what-was-the-cost.html

6. Cybersecurity and Infrastructure Security Agency (CISA). Malware, phishing, and ransomware., on site:
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

7. INTERPOL. Social Engineering & Spear Phishing Threats., on site: https://www.interpol.int/Crimes/Cybercrime

المراجع

8. INTERPOL .When cybercriminals go global, our response must be international, onsite:

https://www.interpol.int/Crimes/Cybercrime.

9. IBM. (2025). Cost of a Data Breach Report. Retrieved from https://www.ibm.com/reports/dawta-breach

10. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware

11. Kaspersky. Ransomware WannaCry: All you need to know, on site:

https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

12. Kosinski, Matthew. IBM. What is phishing?, on site:

https://www.ibm.com/think/topics/phishing

13. Kosinski, Matthew. IBM. What is ransomware?, on site:

https://www.ibm.com/think/topics/ransomware

14. National Cyber Security Centre. Password policy: Updating your approach., November 2018, on site:

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466798 - 51045944

academy@ncsa.gov.qa