CyberEco

مَعًا لِدَعْـم السَّلامة الرَّقميَّة

Together to support digital safety

هُجُوم التَّصيُّد الاحْتِيَالي

شرائح العَرْض

حَقِيبَة خاصَّة بالمُدَرِّب

المرحلة الإعداديَّة

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

حُقُوق المِلْكِيَّة الفِكْرِيَّة

المـادَّة مَمْلُوكـة للوكالـة الوطنيَّـة للأمـن السِّـيبرانيّ فـي دولـة قطـر، وكافَّـة حقـوق المِلكيَّـة الفكريَّـة التـي تشـمل حـقّ المؤلِّـف وحقـوق التَّأليـف والنَّشـر والطِّباعـة، كُلّهـا مكفولـة للوكالـة الوطنيَّـة للأمـن السِّـيبرانيّ فـي دولـة قطـر. وعليه، فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نَشْر أيّ أجزاء من هذه المادَّة، أو الاقتباس منها، أو نَسْخ أيّ جُزْء منها، أو نَقْلها كليًّا أو جزئيًّا في أيّ شكلٍ وبأيّ وسيلة، سواءٌ بطرق إلكترونيَّة أو آليَّة، بما في ذلك التَّصوير الفوتوغرافيّ، أو التَّسجيل، أو استخدام أيّ نظام مِن نُظُم تخزين المعلومات واسترجاعها سواءٌ من الأنظمة الحاليَّة أو المُبْتَكَرَة في المُسْتَقبَل؛ إلَّا بعد الرُّجُوع إلى الوكالة، والحُصُول على إذن خطّيّ منها.

ومَن يُخالف ذلك يُعرِّض نفسه للمُساءَلة القانونيَّة.

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

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

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تَمْهيد	15 دقيقة
الجانب النَّظريّ من المادَّة	45 دقيقة
عَرْض الفيديوهات التَّدريبيَّة	25 دقيقة
اسْتِراحَة قَصِيرَة	20 دقيقة
حِوَار ونِقَاش مع الطلبة	15 دقيقة
المُدَّة الزَّمنيَّة للوَرْشَة	ساعتان

فهرس المحتوى العِلْمِيّ

الفَصْل الأوَّل
مفهوم التَّصيُّد الاحْتِيَالِيّ وأنواعه

أوَّلًا
مفهوم التَّصيُّد الاحْتِيَالِيّ

التَّصيُّد الاحْتِيَاليّ

يُقصَد به تنكُّر المُهاجِمين الإلكترونيِّين في شخصيَّة كيانٍ معروفٍ مثل "جهة حكوميَّة" أو شخصٍ حَسَن السُّمْعَة في رسالة بريد إلكترونيّ أو أيّ شَكْل آخر من أشكال الاتِّصال، وعادةً ما يَستخدم المُهاجِمون رسائل البريد الإلكترونيّ التَّصيُّديَّة لتوزيع الرَّوابِط أو المُرفَقات الضَّارَّة التي من خلالها يَحْصل المُهاجِم على بيانات حسَّاسة تَهُمّ الضَّحيَّة؛ مثل بيانات اعتماد تسجيل الدُّخول، أو أرقام الحسابات البنكيَّة، أو المعلومات الشَّخصيَّة الخاصَّة بالعائلة أو العمل أو غيره.

الهَدف من هجمات التَّصيُّد الاحْتِيَاليّ

01
سرقة المعلومات أو الأموال من المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.

02
تكون بوَّابة لتنفيذ عمليَّات أخرى لتخريب أنظمة المُؤسَّسَات المُسْتَهْدَفة.

03
تثبيت البرمجيات الضَّارَّة على أجهزة المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.

04
دَفْع المُسْتَخْدِم الضَّحيَّة للدُّخول إلى موقع مزيَّف على الإنترنت لإكمال خطَّة الهجوم الاحْتِيَاليّ.

أنــواع
التَّصيُّد الاحْتِيَاليّ

1- التَّصيُّد الاحتياليّ الموجَّه

يُقصَد بالتَّصيُّد الاحْتِيَاليّ الموجَّه استهداف فَرْد ما داخل مُؤسَّسَة مُعيَّنة؛ بغرض سرقة بيانات اعتماد تسجيل الدُّخُول الخاصَّة به؛ حيث يقوم المُهاجِم الإلكترونيّ بجمع المعلومات الشَّخصيَّة عن الفرد المُسْتَهْدَف قبل بَدْء الاحْتِيَال، مثل الاسم والمنصب وتفاصيل الاتِّصال الخاصَّة به.

ويقوم المُهاجِمون الإلكترونيُّون بتنفيذ التَّصيُّد الاحْتِيَاليّ الموجَّه؛ بهدف سرقة الهُويَّة أو الاحْتِيَال الماليّ، أو التَّلاعُب في أسعار الأسهم، أو التَّجسُّس، أو سرقة البيانات السِّرِّيَّة من أجل إعادة بيعها للمُهتمِّين بها، وغالبًا يكونون من المُنافِسِين.

ومن الأفراد المُسْتَهْدَفِينَ بهذا النَّوع من التَّصيُّد الاحْتِيَاليّ: المديرون التَّنفيذيُّون في المُؤسَّسَات الذين قد يفتحون رسائل بريديَّة غير آمِنَة ما يُتِيح للمُجْرمين خرق النِّظَام العامّ للمُؤسَّسَة عبر جهاز المسؤولين.

2- التَّصيُّد الصَّوتيّ

هو أحد أنواع هجمات التَّصيُّد الاحْتِيَاليّ التي يتمّ تنفيذها عبر المكالمات الهاتفيَّة أو البريد الصّوتيّ، بغرض الحصول على أموال الضحايا أو المعلومات الشَّخصيَّة الأخرى.

والسَّبب وراء انتشار هذه الهجمات السيبرانيَّة ما يُعرَف بـ "الهندسة الاجتماعيَّة"، وهي تقنية حديثة تعتمد على الغرائز البشريَّة الطبيعيَّة مثل الثِّقة أو الخوف، وغيرها من مَشاعر يستغلّها المُهاجِمُون السيبرانيُّون للتَّأثير على الضحايا لدَفْعهم إلى اتِّخاذ موقف مُعيَّن يقود إلى تحقيق هدف المُهاجِم مثل سرقة المال أو المعلومات الحسَّاسَة.

وغالبًا ما يتظاهر المُهاجِم الإلكترونيّ بأنَّه أحد الأفراد الذين يعرفهم الضحيَّة أو مسؤول في مصلحة يتعامل معها الضَّحيَّة؛ مثل الجهات الحكوميَّة، أو شركات التأمين، أو البنوك؛ ليبدأ في استدراجه للحصول على المعلومات المُهمَّة منه لتنفيذ باقي خطَّة الاحتيال.

3- التَّصيُّد عبر البريد الإلكترونيّ

في هذا النَّوع من عمليَّات التَّصيُّد الاحْتِيَاليّ؛ يعتمد المُهاجِم السّيبرانيّ على البريد الإلكترونيّ لتنفيذ هجومه على الضَّحيَّة؛ حيث يرسل رسالة بريديَّة تبدو كأنها من مَصْدرٍ موثوقٍ به؛ بهدف التَّسَلُّل إلى الجهاز لسرقة البيانات الحسَّاسَة، أو سرقة المال، أو سرقة الهُويَّة واستغلالها فيما بعد في جرائم أخرى مثل هجوم الفِدْيَة.

علامات تُمَيِّز الرَّسَائل البريديَّة التَّصيُّديَّة

أسـلوب الكتابـة

إذا حَمَلت الرِّسَالة اسم شخصيَّة قريبة من الضَّحيَّة؛ فمن المُستبعَد أن يتمّ التَّحدُّث بصيغة رسميَّة؛ وإذا كانت الرِّسَالة بهذا الأسلوب تتزايد احتماليَّة أن تكون رسالة احْتِيَاليَّة.

الأخطاء النّحويَّة والإملائيَّة

إذا كانت الرِّسَالة تدَّعي أنَّها من مُؤسَّسَة معروفة مثل جوجل Google؛ فإن أغلب المُؤسَّسَات الكبرى تمتلك ميزة التَّدقيق الإملائيّ والنّحويّ لرسائلها البريديَّة، وهو ما يُميِّز رسائلها عن غيرها.

التَّناقض في عناوين البريد الإلكترونيّ والرَّوابِط

يُعدّ البحث عن التَّناقُض في عناوين البريد الإلكترونيّ والرَّوابِط إحدى وسائل كشف الرَّسَائل الاحْتِيَاليَّة، فمثلًا على المُسْتَخْدِم مُطابَقة عنوان البريد الإلكترونيّ الوارد من مُؤسَّسَة كبيرة مثل Google مع العنوان الأصليّ المُعلَن في مَوقعها الرَّسميّ.

علامات تُمَيِّز الرَّسَائل البريديَّة التَّصيُّديَّة

الإلحـاح وإثـارة مَشاعـر الخـوف

غالبًا يلجأ المُهاجِمُون الإلكترونيُّون إلى التَّلاعُب بمشاعر الضَّحايا عبر إثارة الخوف والقلق لديهم حِيَال تعامُلاتهم البنكيَّة أو معلوماتهم الشَّخصيَّة ويبدؤون في طلب بيانات حسَّاسة منهم والإلحَاح بطلب تلك البيانات والمعلومات بصورة عاجِلة.

المُرفَقَـات المَشْبُوهـة

في حال استلام بريد إلكترونيّ يتضمَّن مُرفَقات من مصادر مجهولة، يجب الحذر قبل الضَّغْط عليها، والبحث عن المصدر في مُحرِّكات البحث للتَّأكُّد من وجوده.

طلب تحميـل برامج وروابط

إذا كانت رسالة البريد الإلكترونيّ تدَّعي أنَّها من جهةٍ ما معروفة، وتطلب تثبيت برامج مُعيَّنة أو روابط على الأجهزة، يجب التَّيقُّظ؛ ففي الأغلب تكون رسائل احْتِيَاليَّة.

علامات تُمَيِّز الرَّسَائل البريديَّة التَّصيُّديَّة

رسائـل الجوائـز

في أغلب عمليَّات الاحْتِيَال يتسلَّم الضَّحيَّة رسالة بريديَّة تَدفعه إلى الرَّدّ لتلقّي جوائز ماليَّة كبيرة أو هدايا عينيَّة، ولها وقتٌ محدَّد يجب اللّحاق به، رغم عدم اشتراكه في أيّ مُسابقة مِن قبل؛ ما يعني أن هذا النَّوع من الرَّسَائل احْتِيَاليّ.

تزييـف صفحـات الويـب

قد يقوم المُهاجِم بإنشاء صفحة مُزيَّفة، ثم توجيه رابط منها إلى الضَّحايا للظُّهور بمظهرٍ رَسميّ موثوق به؛ لدَفْعه إلى إجراءٍ ما؛ مثل زيارة الصَّفحة والتَّسجيل فيها أو الضَّغْط على رابطها للوقوع في الفَخّ.

استهداف المُوظَّفين في المُؤسَّسَات

قد يتلقَّى المُوظَّفون في المُؤسَّسَات رسائل بريديَّة تصيُّديَّة بهدف إلحاق الضَّرر بالمُؤسَّسَة أو الدُّخُول إلى نظامها، والتَّلاعُب وسرقة بيانات العملاء، واستغلالها أو بيعها لجهات أخرى خارجيَّة.

4- التَّصيُّد الاحْتِيَالِيّ عَبْر HTTPS

يتمّ عن طريق إرسال رسالة بريد إلكترونيّ إلى المُسْتَخْدِم المُسْتَهْدَف تتضمَّن رابطًا إلى موقع ويب مُزيَّف، بهدف خداع الضَّحيَّة لإدخال معلوماته الخاصَّة، وهذا النَّوْع من الهجمات الاحْتِيَاليَّة يُوصَف بأنَّه مُنخفِض المَخاطِر ومُرتفع المَكاسِب.

5- الهجوم الاحْتِيَالِيّ المعروف بـ Pharming

كلمة Pharming هي عبارة عن مزيج من الكلمتين "Phishing" و"Farming"، وهي عمليَّة احتيال عبر الإنترنت تُشبه التَّصيُّد الاحْتِيَالِيّ؛ حيث يتمّ تصميم موقع ويب مُزيَّف مُشابِه للموقع الرَّسمي المعروف، ثم إعادة توجيه المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ إليه لسرقة المعلومات السِّرِّيَّة.

6- التَّصيُّد الاحْتِيَالِيّ المنبثق Pop-up Phishing

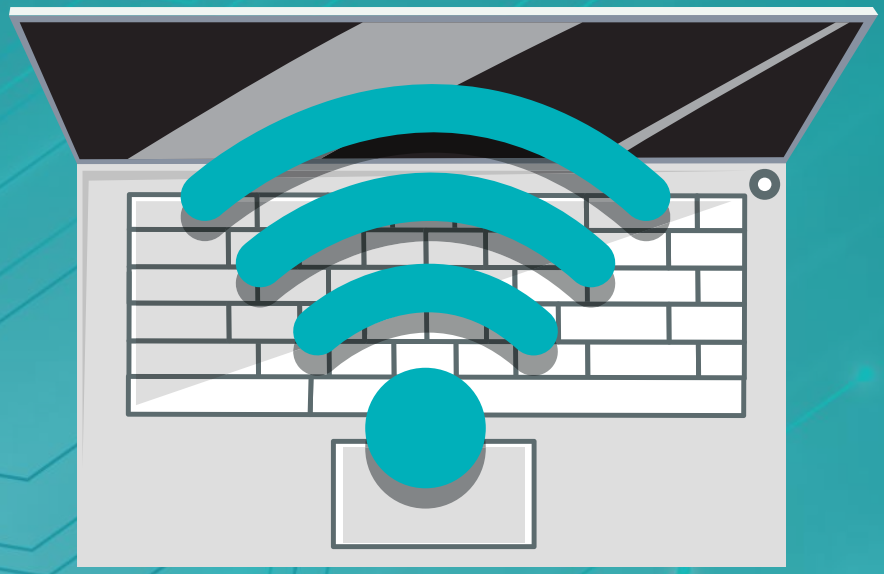
يُقصَد به ظهور رسائل احْتِيَالِيَّة للمُسْتَخْدِمِينَ في أثناء تصفُّحهم لشبكة الإنترنت؛ حيث يصيب المُهاجِمون مواقع الويب الأصليَّة ببرمجيات ضارَّة ما يتسبَّب في ظهور هذه الرَّسَائل المنبثقة عند زيارتها.

خطوات تجنُّب هجمات التَّصيُّد الاحْتِيَاليّ المنبثقة

- وجود برامج مكافحة البرمجيَّات الخبيثة على جهازك يَحدّ من ظهور الرسائل المنبثقة الاحتياليَّة، وفي حال ظهور هذه الرَّسائل يكون الموقع الذي تزوره مصابًا بتلك البرمجيّات الخبيثة، ولا بد من مغادرته فورًا.
- ينبغي عدم مَنْح أيّ شخص إمكانيَّة الوصول عن بُعْد إلى جهاز الحاسوب الخاصّ بك.
- في حال الشَّك بمدى مصداقيَّة الرَّسَائل التي تراها، عليك التَّواصُل مُباشَرة مع مالك الموقع أو فريق الدَّعْم الخاصّ به.

7- تصيُّد التَّوْأم الشِّرير

هو هجوم سيبرانيّ يعمل على خداع المُسْتَهْدَفِينَ للاتِّصال بشبكة Wi-Fi مُزيَّفة تُشبه الأصليَّة، وعند الاتِّصال يبدأ المُهاجِم بالتَّجسس على المعلومات التي يتم إرسالها واستقبالها ثم يقوم بالتَّسلل إلى الأجهزة الخاصَّة بالضَّحايا لسرقة كلّ ما عليها من بيانات وملفَّات.



خطوات تنفيذ الهجوم الإلكترونيّ

- اختيار مكان عامّ يَتضمَّن خدمة Wi-Fi مجانيَّة: مثل المطارات والمكتبات العامَّة أو المقاهي لبَدْء الهجوم.
- إعداد نقطة وصول Wi-Fi: يقوم المُهاجِم بإنشاء نقطة اتِّصال جديدة باستخدام اسم مألوف لتسهيل مهمَّة جذب المُسْتَخْدِمِينَ للشبكة والبَدْء في استخدامها.
- إنشاء صفحة بوّابة تسجيل مُقيَّدة مُزيَّفة: يضع المُهاجِم بوَّابة على شبكة Wi-Fi العامَّة، والتي تطلب من المُسْتَخْدِمِينَ كلمات مرور أو معلومات شخصيَّة للمرور إلى الشبكة.
- الاقتراب من الضَّحايا: بعد قيام المُهاجِم بالخطوات السَّابقة يبدأ في توجيه أجهزته بالقرب من الضَّحايا المحتملين لإنشاء إشارة أقوى، وبالتَّالي يختارون الشَّبكة المُزيَّفة لاستخدامها ما يُوقِعُهم في الفَخّ.
- مُراقَبَة وسرقة بيانات المُستخْدِم: بعد دخول المُسْتَخْدِم المُسْتَهْدَف للشَّبكة يبدأ المُهاجِم بمُراقبة ما يقوم به عبر الإنترنت، ويجمع البيانات من أرقام ومعلومات مُهمَّة.

8- التَّصيُّد الاحتياليّ المُوجَّه لكبار الشَّخصيَّات

هو هجوم تَصيُّد احْتِيَاليّ يَستهدف كبار المسؤولين التَّنفيذيِّين في المُؤسَّسَات، ويأتي مُتنكِّرًا في صورة رسالة بريد إلكترونيّ مألوفة، وهو مُصمَّم على تحفيز ضحاياه على القيام بإجراءات مثل تحويل الأموال أو إرسال بيانات شخصيَّة.

وتُعدّ المُؤسَّسَات الماليَّة وخدمات الدَّفْع هي الأكثر استهدافًا من هذا النَّوْع من هجمات التَّصيُّد الاحْتِيَاليّ، إذ تحتوي على معلومات شخصيَّة حول المُؤسَّسَات أو الأفراد النَّافذين المُسْتَهْدَفِينَ.

أهداف التَّصيُّد الاحتياليّ المُوجَّه لكبار الشَّخصيَّات

1

دَفْع الضَّحايا للنَّقْر على روابط لمواقع تتضمَّن برمجيات ضارَّة.

2

طلب تحويل الأموال إلى الحساب المصرفيّ للمُهاجِم السّيبرانيّ.

3

طلب بيانات خاصَّة بالمُؤسَّسَات أو الأفراد لشَنّ المزيد من الهجمات مثل هجوم الفِدْيَة.

الأضرار النّاتجة عن التّصيُّد الاحتياليّ المُوجّه لكبار الشّخصيّات

01 فُقْدَان البيانات

بمُجَرَّد الضَّغْط على الرَّوابِط أو تنزيل مُرفَقات البريد تبدأ الشَّبكات الدَّاخليَّة بالإصابة بالبرمجيَّات الضَّارَّة التي تُمكِّن المُتَسَلِّلين من الدُّخُول وسرقة ما يرغبون فيه من بيانات.

02 تضرُّر سمعة المُؤسَّسَات والأفراد

قد يُؤدِّي فُقْدَان البيانات إلى إلحاق خسائر ماليَّة كبيرة بالمُؤسَّسَات والأفراد، فضلًا عن تضرُّر سُمْعتها أمام الجهات الرَّسميَّة في الدّولة التي سنَّت تشريعات لحماية البيانات.

9- استنساخ التَّصيُّد Clone Phishing

يُقصَد به قيام أحد المُتَسَلِّلين بعمل نُسخة مُطابِقَة من الرِّسَالة التي استلمها المُستلِم بالفِعْل. وقد تتضمَّن شيئًا مثل عبارة "إعادة إرسال هذا"، مع وَضْع رابط ضارّ في البريد الإلكترونيّ.

10- التَّصيُّد الخادع Deceptive Phishing

يستخدم المُهاجِمُون الإلكترونيُّون تقنية خادعة للتَّظاهُر بأنَّهم يعملون مع شركة حقيقيَّة، مثل شركة أبل Apple؛ لإبلاغ المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ بأنَّهم يَتعرَّضُون بالفعل لهجوم إلكترونيّ، لدَفْعهم للنَّقْر على رابطٍ مُعيَّن، لكنَّه في الحقيقة ضارّ ما يتسبَّب في إصابة الحواسيب الخاصَّة بهم.

الفَصْل الثَّاني
كيفيَّة تنفيذ هجمات التَّصيُّد الاحْتِيَاليّ

الثَّغَرات التي يستغلّها مُنَفِّذُو هجمات التَّصيُّد الاحْتِيَاليّ

طُرُق يستغلّها المُهاجِمون السيبرانيُّون لخرق أجهزة المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ:

إرسال رسائل نصيَّة أو رسائل بريد إلكترونيّ مُزيَّفة تحتوي على روابط تتضمَّن برمجيات ضارَّة.

يحتال المُهاجِمون عبر الادِّعاء بتقديم الدَّعْم الفنِّيّ؛ حيث يتَّصلون بالمُسْتَخْدِم المُسْتَهْدَف عبر رسائل البريد الإلكترونيّ أو المحادثات مُدَّعين أنَّ الجهاز تعرَّض للخرق.

عدم تحديث المُسْتَخْدِمِينَ للبرامج والتَّطبيقات يجعل منها منفذًا أمام المُهاجِمين للتَّسلُّل إلى الأجهزة الشَّخصيَّة.

استخدام كلمات مرور ضعيفة أو سهلة التَّخمين على الأجهزة وشبكة Wi-Fi الخاصَّة بالمُستخْدِم.

النَّقْر على الرَّوابِط المجهولة أو غير الموثوق بها مِن قِبَل المُسْتَخْدِمِينَ.

علامات تُؤكِّد تعرُّض الأجهزة الإلكترونيَّة للخَرْق

- تلقِّي إشعارات عبر البريد الإلكترونيّ حول محاولات تسجيل الدُّخُول على حساباتك رغم عدم قيامك بذلك.
- بُطْء الجهاز، وارتفاع حرارته، وتأخُّر تنفيذ الأوامر التي يتلقَّاها من المُستخْدِم.
- ظهور نوافذ منبثقة تحتوي على رسائل مُزعِجَة تدَّعي إصابة جهازك الإلكترونيّ بالفيروسات.
- فتح نوافذ المُتصفِّح وعلامات التَّبويب والتَّطبيقات الموجودة على جهاز المُسْتَخْدِم الخاصّ من تلقاء نفسها.
- تلقِّي اتِّصال تحذيريّ من مكان العمل حول خَرْق البيانات.
- محاولات تسجيل دخول غير ناجحة إلى حساباتك.
- تلقِّي الأصدقاء وزملاء العمل رسائل غير مألوفة من المُسْتَخْدِم المُسْتَهْدَف.
- تلقِّي رسائل بريد عشوائي في صندوق الوارد الخاصّ بك.
- إعادة توجيه المُسْتَخْدِم المُسْتَهْدَف باستمرار إلى مواقع الويب غير المرغوب فيها في أثناء محاولته تصفُّح الإنترنت.

الأخطاء التي يرتكبها مُسْتَخْدِمُو الإنترنت

1. التَّصفُّح على شبكة Wi-Fi عامَّة دون اتِّخاذ الاحتياطات الأمنيَّة المطلوبة؛ ما يجعلهم أكثر عُرْضَة للخَرْق والوقوع ضحيَّة لهجمات التَّصيُّد الاحْتِيَاليّ.
2. عدم تحديث المُتصَفِّح والتَّطبيقات الموجودة على الأجهزة.
3. مُشارَكة الكثير من المعلومات الشَّخصيَّة على وسائل التَّواصُل الاجْتِمَاعيّ.
4. تشابُه كلمات المرور لعددٍ من الحسابات عبر الإنترنت.
5. استخدام كلمات مرور سَهْلة التَّخمين.
6. عدم تثبيت برامج الحِمايَة من البرمجيَّات الخبيثة.

الأخطاء التي يرتكبها مُسْتَخْدِمُو الإنترنت

7 فَتْح الرَّوابِط من رسائل البريد الإلكترونيّ دون التَّحقُّق من موثوقيتها.

8 الانسياق وراء الرَّسَائل البريديَّة التي تحتوي على استطلاعات أو فُرَص هدايا أو مسابقات، دون التَّحقُّق من صِحّتها عبر البحث على مُحرّكات مثل جوجل Google عن اسم الشَّركة.

9 تجاهُل ميزات الأمان الأساسيَّة، ومن بينها المُصادَقة الثنائيَّة.

10 التَّسوُّق عبر الإنترنت يزيد من فُرَص تَعرُّض المُسْتَخْدِم للخَرْق، خاصَّةً إذا استخدم بطاقاته البَنْكيَّة الشَّخصيَّة.

11 يَنْتشر على وسائل التَّواصُل الاجْتِمَاعيّ -خاصَّةً Facebook- الكثير من الاختبارات المُغْرِيَة وبمُجرَّد زيارة المُسْتَخْدِم لهذه الصَّفحات يُصبح فريسةً للاحتيال والسَّرقة.

12 عدم الاستفادة من إعدادات الخُصُوصيَّة الخاصَّة بك على وسائل التَّواصُل الاجْتِمَاعيّ.

البَصْمَة الرَّقميَّة
والتَّصيُّد الاحْتِيَاليّ

البَصْمَة الرَّقميَّة (الإلكترونيَّة)

هي مَسار البيانات التي يَتركها المُسْتَخْدِم عند استخدام شبكة الإنترنت، مثل المواقع التي يزورها ورسائل البريد الإلكترونيّ وعمليَّات التَّسوُّق والمحادثات (الدردشات) وجميع التَّحرُّكات التي يقوم بها المُسْتَخْدِم عبر حساباته المختلفة أيًّا كانت تلك التَّحرُّكات؛ جَيِّدة أم لا.

وقد تساهم مواقع الإنترنت في تشكيل بَصْمَة المُسْتَخْدِم الرَّقميَّة؛ من خلال تثبيت "ملفَّات تعريف الارتباط" (Cookies) على أجهزته، كما يمكن للتَّطبيقات جَمْع البيانات الخاصَّة بالمُسْتَخْدِمِينَ دون علمهم، وذلك في حال سَمحوا لها بالوصول إلى الملفَّات المُخزَّنة؛ سواءٌ كانت نصيَّة أو فيديوهات أو صورًا أو غير ذلك.

البَصْمَات الرَّقميَّة النَّشِطة

يُقصَد بها قيام المُسْتَخْدِم عمدًا بنَشْر المعلومات والبيانات الخاصَّة به علنًا؛ مثلما يحدث على وسائل التَّواصُل الاجْتِمَاعيّ، أو تسجيل الدُّخُول إلى مواقع الإنترنت من خلال البيانات التعريفيَّة، مثل (اسم المُسْتَخْدِم وكلمة السِّرّ)، أو إكمال نموذج بيانات عبر الإنترنت مثلما يحدث عند الاشتراك في الخدمات الإخباريَّة أو الوظائف أو غيرها.

البَصْمَات الرَّقميَّة الخَامِلَة

يُقصَد بها ما يَتِمّ جَمْعه من معلومات عن المُسْتَخْدِمِينَ دون عِلْمهم، مثل تجميع مواقع الإنترنت لمعلومات عن عدد الزِّيارات والصَّفحات التي تمَّت زيارتها، وعدد المُشاهَدات على أحد الفيديوهات وعناوين IP، وكذلك استفادة الجهات الإعلانيَّة من تسجيلات الإعجاب والمُشارَكات والتَّعليقات التي يقوم بها المُسْتَخْدِم بشكلٍ عَفويّ من أجل تَوجيه محتويات تتناسب مع اهتماماته فيما بعد.

أهميَّة البَصْمَة الرَّقميَّة

1. تكون دائمةً، ويصعب السَّيطرة على كيفيَّة استخدام الآخرين لها.
2. تُحدِّد السُّمْعَة الرَّقميَّة للمُستخدِم.
3. يمكن لأصحاب العمل والجامعات التَّحقُّق من البَصْمات الرَّقميَّة للمُوظَّفين والطَّلبة المُحتَمَلِين.
4. يمكن إساءة تفسير الكلمات والصُّور ومقاطع الفيديو التي تتمّ مشاركتها.
5. الإضرار بالعلاقات الاجتماعيَّة بين الأفراد.
6. يمكن للمُتَسَلِّلين الإلكترونيِّين استغلال البَصْمَة الرَّقميَّة في عمليَّات التَّصيُّد الاحْتِيَاليّ أو في إنشاء هُويَّات مُزيَّفة.

طُرُق تشكيل البَصْمَة الرَّقميَّة

1. التَّسوُّق عبر الإنترنت.
2. التَّسجيل في النَّشرات البريديَّة بالمواقع الإلكترونيَّة.
3. المعاملات الماليَّة عبر الإنترنت.
4. وسائل التَّواصُل الاجْتِمَاعيّ.
5. الانضمام إلى المواقع الإلكترونيَّة.
6. الاشتراك في النَّشرات الإخباريَّة.
7. الاشتراك في التَّطبيقات المختلفة.

حماية البَصْمَة الرَّقميَّة

1. التَّحقُّق من البَصْمَة الرَّقميَّة الخاصَّة بالمُستخْدِم عَبْر مُحرِّكات البحث.
2. إزالة المعلومات الشَّخصيَّة من المواقع غير المُهمَّة.
3. السَّيطرة على كميَّة المعلومات التي تتمّ مُشاركتها عبر وسائل التَّواصُل الاجْتِمَاعيّ وباقي المواقع.
4. ضَبْط إعدادات الخُصُوصيَّة.
5. التَّحقُّق من المواقع التي تتمّ زيارتها أو تصل روابطها على البريد الإلكترونيّ.
6. تجنُّب استخدام شبكات Wi-Fi عامَّة.

حماية البَصْمَة الرَّقميَّة

7 حَذْف الحسابات القديمة.

8 إنشاء كلمات مرور قويَّة ومختلفة للحسابات.

9 عدم تسجيل الدُّخُول إلى المواقع أو التَّطبيقات بواسطة بيانات Facebook.

10 تحديث البرامج والتَّطبيقات أولًا بأول.

11 تعيين كلمة مرور للهاتف الذَّكيّ.

12 عند التَّعرُّض للخَرْق يجب تغيير كلمات المرور لجميع الحسابات فورًا.

الفَصْل الثَّالث

كيفيَّة التَّصرُّف في حال التَّعرُّض لتَصيُّد احْتِيَاليّ

إرشادات الحماية من التَّصيُّد الاحْتِيَالِيّ

01

ينبغي تجنُّب النَّقْر على الرَّوابِط أو المُرفَقات المُرْسَلة في رسائل البريد الإلكترونيّ مجهولة المصدر أو غير المُتَوَقَّعة.

02

في حال تلقّي إشعارات مُتكرِّرة عن محاولة تسجيل الدُّخُول لحسابات المُسْتَخْدِم، عليه تغيير كلمة المرور فورًا في جميع الحسابات؛ بشرط أن تكون الكلمة قويَّة وطويلة.

علامات تُمَيِّز رسائل البريد الإلكترونيّ الاحْتِيَاليَّة

1

تحتوي الرَّسَائل على لُطْف مُبالَغ به.

2

تدعو الرَّسَائل المُسْتَخْدِم للنَّقْر على رابطٍ لتحديث تفاصيل الحسابات الخاصَّة به بصورة عاجلة.

3

كثرة الأخطاء الإملائيَّة والنحويَّة برسائل البريد.

كيف تحمي نفسك من هجمات التَّصيُّد؟

لا تفيد دائمًا عمليَّة تصفية البريد العشوائيّ في التَّخلُّص من جميع الرَّسَائل الاحْتِيَاليَّة بسبب تَحايُل المُهاجِمين للوصول إلى المُستخْدِم، ومن طُرُق الحماية:

01

استخدام برامج الأمان والحماية من البرمجيَّات الضارة ومُكافحة الفيروسات لحماية أجهزة الحاسوب، مع تعيين التَّحديث التّلقائيّ للبرامج والتَّطبيقات لتتمكَّن من مُواجَهة التَّهديدات السيبرانيَّة.

02

وَضْع كلمة مرور قويَّة للهاتف الذَّكيّ مع ضَبْط التَّحديث التِّلقائيّ للبرامج عليه.

03

استخدام المُصادَقة الثُّنائيَّة لتوفير أمانٍ إضافيّ للحسابات، سواءٌ بواسطة رمز المرور أو كلمات السر ذات الاستخدام الواحد OTP أو الإجابة عن سؤال رَمْز المرور أو الإجابة عن سؤالٍ ما، أو ببصمة الإصبع أو الوَجْه.

04

عمل نُسْخة إضافيَّة من البيانات المُخزَّنة، ووَضْعها في مكانٍ آخر بخلاف أجهزة الحاسوب لإمكانيَّة استرجاعها إذا تعرَّض الجهاز للخَرْق.

طرق حماية البيانات من القَرْصَنَة

- استخدام برامج مُكافَحة الفيروسات؛ فهي تُمثِّل خطّ الدِّفاع الأوَّل ضدّ الهجمات الاحْتِيَاليَّة.
- تفعيل المُصادَقة الثُّنائيَّة؛ فهي الطريقة المُثلى لحماية الحسابات من الدُّخُول غير المُصرَّح به وسرقة البيانات.
- تحديث البرامج والتَّطبيقات أمرٌ ضروريّ؛ نظرًا لإدخال تعديلات دائمة عليها مِن قِبَل الشَّركات التكنولوجيَّة المُنْتِجَة لسَدّ أيّ ثغرات أمنيَّة تظهر بها.
- يجب وضع نُسْخة احتياطيَّة من البيانات في مكانٍ آخر بعيدًا عن الجهاز الشَّخصيّ؛ لحمايتها في حال تمَّ خَرْق الجهاز أو حالات الضَّياع أو الإتلاف.

- التَّثقيف بمبادئ الأمن السّيبرانيّ، تسهم تلك الخطوة في حماية الأفراد من الوقوع في فخّ التَّصيُّد الاحْتِيَاليّ، وغيرها من هجمات سيبرانيَّة هدفها الأساسيّ إلحاق الضَّرر بمُستخْدِمي الإنترنت.
- تجنُّب استخدام شبكة Wi-Fi عامَّة (مجانيَّة) قَدْر الإمكان على الجهاز الشَّخصيّ.
- التَّحقُّق من الرَّوابِط المُرسَلَة بالبريد قَبْل النَّقْر عليها.
- إيقاف تشغيل Bluetooth على الجهاز الشَّخصيّ في حال عدم الحاجة إليه.
- تقليل البَصْمَة الرَّقميَّة، وتفعيل إعدادات الخصوصيَّة لوسائل التَّواصُل الاجْتِمَاعيّ.

ماذا أفعل عند تعرضي للتَّصيُّد الاحتياليّ؟

01

في حال شك المُسْتَخْدِم بتعرُّضه لهجوم تصيُّد احْتِيَاليّ مثل رسالة بريد مُزيَّفة، فإذا كان لديه تعامُل مع الأفراد أو الجهات المُدْرَجَة في الرَّسَائل فعليه التَّواصُل معها شخصيًّا عبر الأرقام المُعتمَدَة أو الحسابات الرَّسميَّة.

02

في حال فتح أيّ مُرفَق أو رابط برسالة البريد الإلكترونيّ الاحتيالية التي تَستهدِف المعلومات البنكيَّة، فهنا على المُسْتَخْدِم الاتِّصال بالبنك ووَقْف بطاقته الائتمانيَّة إذا شكَّ أنَّها مُعرَّضة للسَّرقة.

ماذا أفعل عند تعرضي للتَّصيُّد الاحتياليّ؟

03

في حالة خَرْق جهاز الحاسوب الخاصّ بالمُسْتَخْدِم فهنا عليه التَّحرُّك سريعًا، وفَصْل الاتِّصال بشبكة Wi-Fi الخاصَّة به، مع تفعيل برامج مُكافَحة الفيروسات للبحث عن البرمجيات الضَّارَّة، وحذف التَّطبيقات المشكوك فيها.

04

ينبغي للمُسْتَخْدِم في هذه الحالات تحديث أنظمة التَّشغيل الخاصَّة به، وإعادة تعيين كلمات المرور جميعها، وتفعيل المُصادَقة الثُّنائيَّة، ومسح الجهاز والبدء في التَّثبيت من جديد.

ماذا أفعل عند تعرضي للتَّصيُّد الاحتياليّ؟

05

تحذير الأصدقاء وأفراد العائلة وزملاء العمل والمدرسة من إمكانيَّة تلقّيهم رسائل احْتِيَاليَّة من خلال تعرُّضك للخَرْق، وذلك لتَجْنيبهم التَّعرُّض لهجمات التَّصيُّد الاحْتِيَاليّ.

06

إجراء فَحْص مُتقدّم دون الاتِّصال بالإنترنت بواسطة برنامج الأمان المُدْمَج في نظام ويندوز Windows، من خلال فَتْح الإعدادات الخاصَّة بالمُسْتَخْدِم على جهاز الحاسوب والانتقال إلى قائمة إعدادات الأمان، ثمَّ تحديد "الحماية من الفيروسات والتَّهديدات"؛ للبدء في إجراء فَحْص شامل لمُكافَحة الفيروسات وغيرها من بَرمجيَّات خبيثة على الجهاز دون الحاجة للاتِّصال بالإنترنت.

ماذا أفعل عند تعرضي للتَّصيُّد الاحتياليّ؟

07

يمكن الاستفادة من خدمات الدَّعْم الفنِّيّ المُقدَّمَة من شركات التكنولوجيا مثل مايكروسوفت Microsoft عبر الاتِّصال بالرَّقم المعتمَد أو وسائل الاتِّصال المُعلَن عنها، والأمر نفسه لباقي الشَّركات التقنيَّة مثل أبل Apple.

08

التَّواصُل مع إدارة مُكافَحة الجرائم الإلكترونيَّة بوزارة الداخليَّة عند التَّعرُّض لأحد أنواع التَّصيُّد الاحْتِيَاليّ لامتلاك هذه الجهات الأجهزة والكفاءات التي تُمكِّنها من التَّدخُّل ومُعالَجة المشكلة قبل تفاقمها، واستعادة البيانات وتَوقيف المُتَسَلِّلين السّيبرانيِّين.

التمارين والتدريبات

أولًا: التَّمَارين الصَّفِّيَّة

انْتَبِه!

التَّصيُّد الاحْتِيَالِيّ

يُقصَد به تنكُّر المُهاجِمين الإلكترونيّين في شخصيَّة كيان معروف أو شخص حَسَن السُّمْعَة في رسالة بريد إلكترونيّ أو أيّ شكلٍ آخر من أشكال الاتِّصال، وعادةً ما يَستخدم المُهاجِمون رسائل البريد الإلكترونيّ التَّصيُّديَّة لتوزيع الرَّوابِط أو المُرفَقَات الضَّارَّة التي من خلالها يحصل المُهاجِم على بيانات حسَّاسة تهمّ الضَّحيَّة مثل بيانات اعتماد تسجيل الدُّخُول، أو أرقام الحسابات البنكيَّة، أو المعلومات الشَّخصيَّة الخاصَّة بالعائلة أو العمل...وهكذا.

هل تعلم؟

التَّصَيُّد الصَّوتيّ أحد أنواع هجمات التَّصَيُّد الاحتياليّ التي يتمّ تنفيذها عبر المكالمات الهاتفيَّة؛ بغرض الحصول على أموال الضَّحايا أو المعلومات الشَّخصيَّة الأخرى.

انْتَبِه!

التَّصيُّد الاحتياليّ الموجَّه

يُقصَد بالتَّصيُّد الاحتياليّ الموجَّه استهداف فَرْد ما داخل مُؤسَّسَة مُعيَّنة؛ بغرض سرقة بيانات اعتماد تسجيل الدُّخُول الخاصَّة به؛ حيث يقوم المُهاجِم الإلكترونيّ بجمع المعلومات الشَّخصيَّة عن الفرد المُسْتَهْدَف قبل بَدْء الاحْتِيَال مثل الاسم والمنصب وتفاصيل الاتِّصال الخاصَّة به. ومن الأفراد المُسْتَهْدَفِينَ بهذا النَّوع من التَّصيُّد الاحْتِيَاليّ: المديرون التَّنفيذيُّون في المُؤسَّسَات الذين قد يفتحون رسائل بريديَّة غير آمِنَة ما يُتيح للمُجْرمين خَرْق النِّظَام العامّ للمُؤسَّسَة عبر جهاز المسؤولين.

التَّمرين الأوَّل

حدّد **«الصَّحيح»** أو **«الخاطئ»** فيما يتعلّق بالتَّصيُّد الاحتياليّ.

تَوْجيه

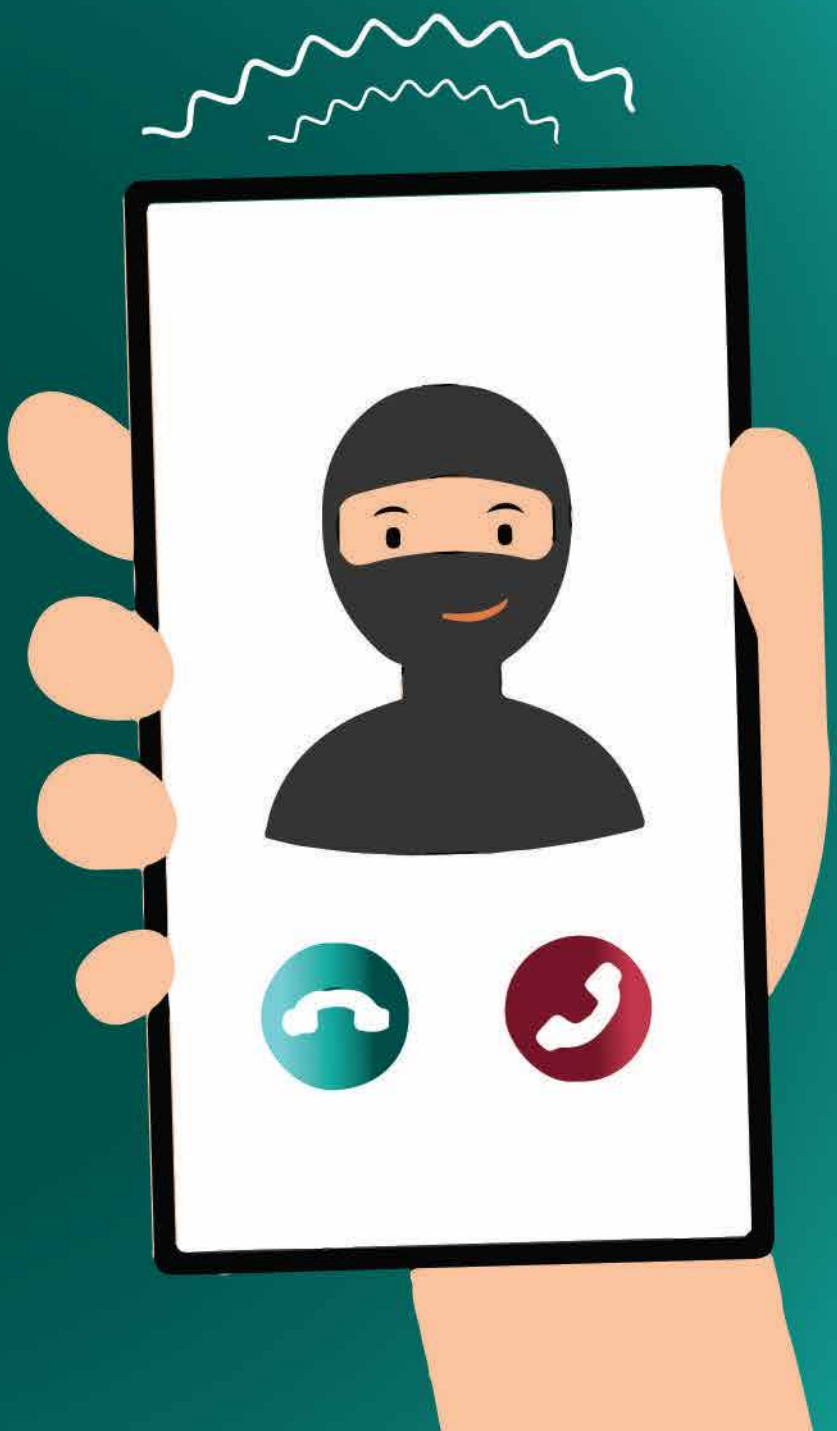
اقرأ العبارات الواردة بتمعُّن، وفكِّر فيما إذا كانت هذه العبارات تُعبّر عن معلومات صحيحة أو خاطئة فيما يتعلّق بالتَّصيُّد الاحتياليّ، ثم وَضع مثال محلول في الجدول.

التَّصيُّد الاحتياليّ هو محاولة لسرقة الأموال أو الهويّات من خلال كشف المعلومات الشّخصيّة.	صحيح
يهتمّ منفذو التَّصيُّد الاحتياليّ بالمعلومات السّرّيّة، مثل منشورات منصّات التّواصل الاجتماعيّ.	
التَّصيُّد الاحتياليّ يعتمد على كشف المعلومات السّرّيّة، التي تشمل أرقام البطاقات الائتمانيّة وكلمات السّرّ والمعلومات البنكيّة.	
أحيانًا تقوم مواقع إلكترونيّة بعمليّات التَّصيُّد الاحتياليّ.	
لا يسْرق منفذو التَّصيُّد الاحتياليّ هُويّة أحَد الأصدقاء أو أفراد الأُسْرة.	
تُستخدَم الرّسائل المزيّفة في عمليّات التَّصيُّد الاحتياليّ.	
الرّوابط المشبوهة من أبرز طرق التَّصيُّد الاحتياليّ.	
لا يمكن لمنفذي التَّصيُّد الاحتياليّ الاستفادة بالمعلومات البنكيّة أو أرقام البطاقات الائتمانيّة.	
لا يهتمّ مُجْرمو التَّصيُّد الاحتياليّ بالهويّة.	
لا يمكنك حماية نفسك من التَّصيُّد الاحتياليّ مهما حاولت.	

انْتَبِه!

التَّصيُّد الصَّوتيّ

هو أحد أنواع هجمات التَّصيُّد الاحْتِيَاليّ التي يتمّ تنفيذها عبر المكالمات الهاتفيَّة أو البريد الصّوتيّ، بغرض الحصول على أموال الضحايا أو المعلومات الشَّخصيَّة الأخرى. والسَّبب وراء انتشار هذه الهجمات الإلكترونيَّة ما يُعرَف بـ "الهندسة الاجتماعيَّة"، وهي تقنية حديثة تعتمد على الغرائز البشريَّة الطبيعيَّة مثل الثِّقة أو الخوف.... وغيرها من مَشاعر يستغلّها المُهاجِمُون الإلكترونيُّون للتَّأثير في الضحايا لدَفْعهم إلى اتِّخاذ موقف مُعيَّن يقود إلى تحقيق هدف المُهاجِم مثل سرقة المال أو المعلومات الحسَّاسَة.



انْتَبِه!

التَّصَيُّد عبر البريد الإلكترونيّ

يعتمد مخترق البيانات على البريد الإلكترونيّ لتنفيذ هجومه على الضَّحيَّة؛ حيث يرسل رسالة بريديَّة تبدو كأنها من مَصْدرٍ موثوقٍ به؛ بهدف التَّسَلُّل إلى الجهاز لسرقة البيانات الحسَّاسَة، أو سرقة المال، أو سرقة الهُويَّة واستغلالها فيما بعد في جرائم أخرى مثل هجوم الفِدْيَة.

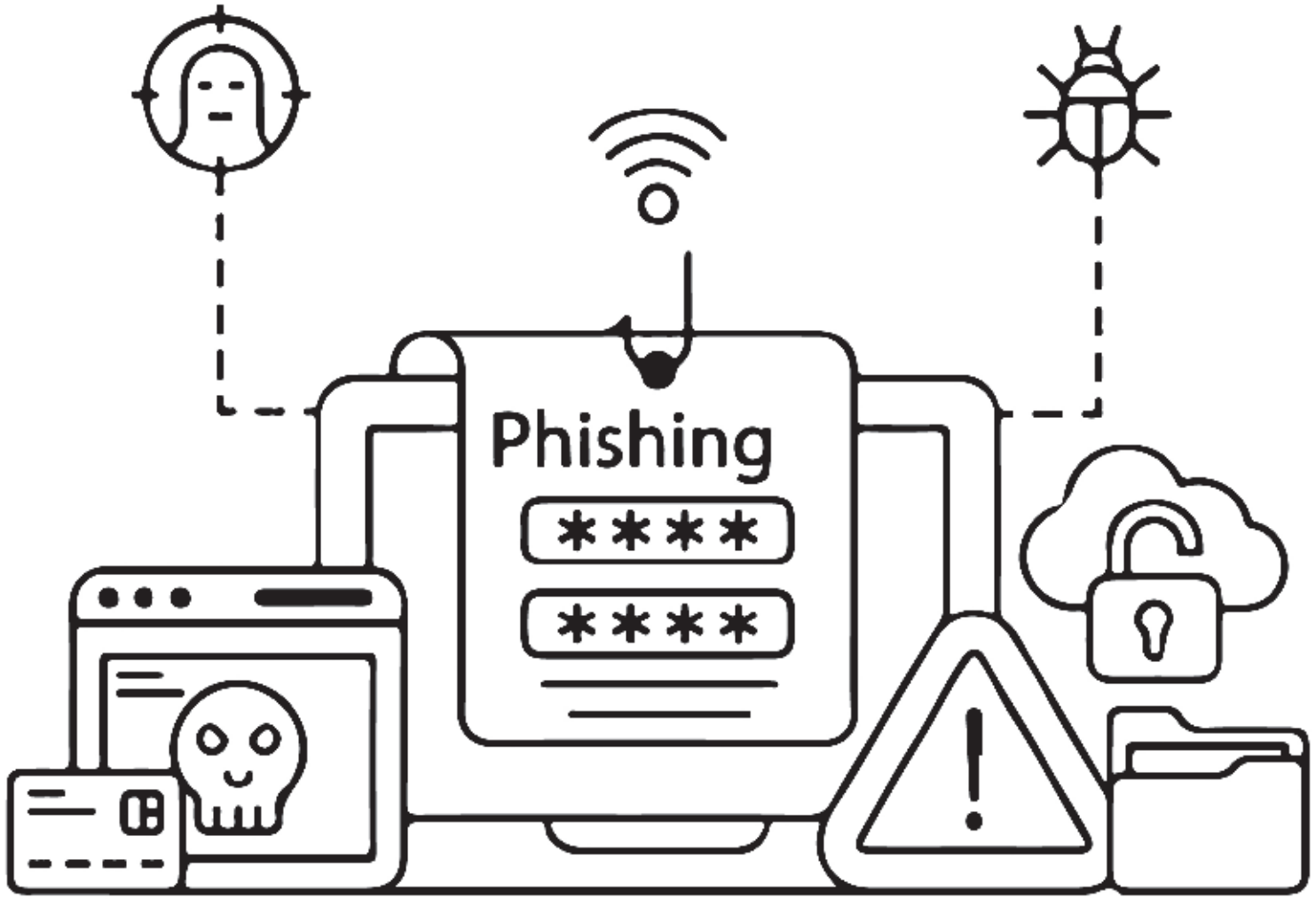
التَّمرين الثَّاني

ضَع الكلمة المناسبة لكلّ تعريف

توجيه

اقْرأ العبارات الواردة أدناه بتَمَعُّن، وفكِّر فيما إذا كانت هذه العبارات تُعبِّر عن معلومات صحيحة أو خاطئة فيما يَتعلَّق بالتَّصَيُّد الاحتياليّ، ثمّ وَضْع مثال محلول في الجدول.

هو الشَّكل الأكثر شيوعًا للتَّصَيُّد الاحتياليّ، ويستخدم برامج البريد الإلكترونيّ للنَّصب والسَّرقة.	**التَّصَيُّد عبر البريد الإلكترونيّ**
نوع من البرمجيَّات الضَّارَّة التي يتمّ إخفاؤها في مُرْفق من المُرْفقات التي تَصِل إليك عبر البريد الإلكترونيّ وبمجرَّد فتحها تتسبَّب في تعطيل أنظمة التَّشغيل.	
نوع من هجمات التَّصَيُّد الاحتياليّ تَستهدِف الشَّبكات الكبيرة، أو مجموعة أشخاص بعينهم من خلال استغلال أبحاث أُجْرِيت عنهم وعن عملهم وحياتهم الاجتماعيَّة.	
تُستخدَم فيه الرَّسائل القصيرة وتأتي متخفِّية في هيئة علامات تجاريَّة أو مواقع كبيرة موثوق بها؛ لخداع المُستخدِم لفتح الرَّابط أو النَّصّ المُرسَل.	
يُستخدَم فيه الصَّوت لدَفْع الضَّحِيَّة للإدلاء بمعلومات حسَّاسة وشخصيَّة عبر الهاتف، من خلال سرقة هويات شخصيات مُقرَّبة من الضَّحايا.	


Phishing
*****
*****

هل تعلم؟

هجمات التَّصَيُّد الاحتياليّ المُوجَّه؛ هجمات واسعة النِّطاق تستهدِف البيانات الحسَّاسة للمُستخدِمين بشَكْلٍ عامّ.

انْتَبِه!

التَّصيُّد الاحْتِيَاليّ عَبْر HTTPS

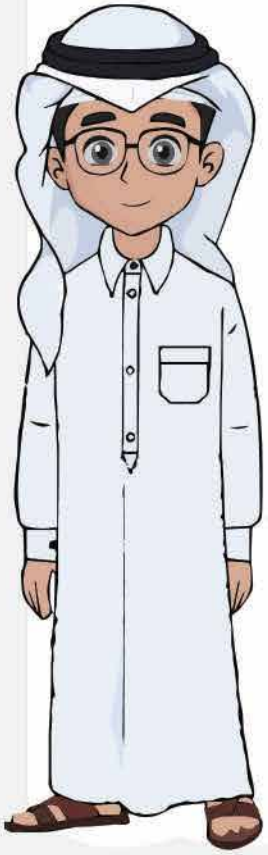
يتمّ عن طريق إرسال رسالة بريد إلكترونيّ إلى المُسْتَخْدِم المُسْتَهْدَف تتضمّن رابطًا إلى موقع ويب مُزيَّف، بهدف خداع الضَّحيَّة لإدخال معلوماته الخاصَّة.

التَّمرين الثَّالث

أكْمِل الجمل التَّالية:

توجيه

اقْرأ العبارات الواردة أدناه بتَمَعُّن، وضَع الكلمات المناسبة في الفراغ بحيث تُصبِح العبارات ذات معنًى مفيد، ثمّ وَضْع مثال محلول في الجدول.



1. يَستخدِم المهاجمون الاتِّصالات من أجل التَّلاعب ..... **بمشاعر الضَّحايا** ..... والحصول على معلومات ..... ويستغلُّون في ذلك عدم وَعْي الضَّحِيَّة أو عدم التَّفكير في المخاطر من تبادل تلك ..... والبيانات.

2. يَحْرِص المُتَصيِّدون على ..... حاجة الضَّحايا من أجل ..... ، وغالبًا ما يَقَع الباحثون عن عملٍ في هذا الفَخّ، فيُسْرِعُون بتسجيل ..... دون التَّحقُّق من الموقع، وبالطَّبع تُسْتَغلّ تلك البيانات ضدَّهم.

3. الثِّقة الزَّائدة من أبرز ..... التي يَقَع فيها الضَّحايا، الذين ينخدعون من ..... المزيَّفة ولا يتأكَّدون من صِحَّة ما يَصِلهم من معلومات.

4. التَّلاعب العاطفيّ أيضًا يُستخدَم لـ ..... الضَّحايا ودفعهم للتَّصرُّف دون ..... أو حذر، ويستغلّ المهاجمون في ذلك مشاعر الخوف و ..... للحصول على ما يريدون دون أيّ عناء.

التَّمرين الرَّابع

رتّب العبارات التّالية وفقًا للتّسلسل المنطقيّ... كيف تحمي نفسك من التصيد الاحتيالي؟

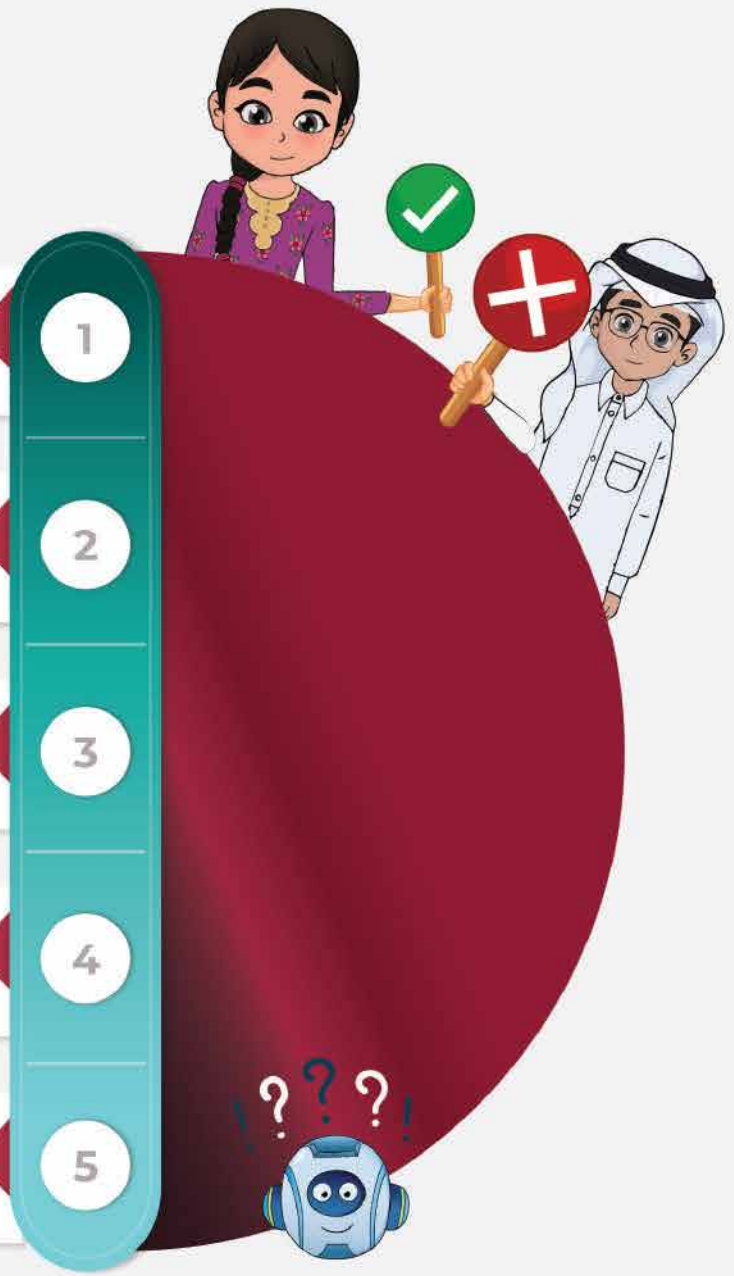
توجيه

اقرأ الجُمَل الواردة في الجدول بتَمَعُّن، وأعِد ترتيب الجُمَل بحيثُ تكون الجُمْلَة الأُولى تُعَبّر عن التّصرُّف الأوّل الّذي يجب أنْ تتصرّفه فور تَعَرُّضِك للتصيد الاحتيالي، والجُمْلَة الثّانية هي التّصرُّف الثّاني، وهكذا.

1	في حالة استخدام اسم شركة أو موقع، عليك التّواصل مع الشّركة وتحذيرها من استخدام اسمها في أعمال وأغراض احتياليّة.	
2	توجّه فورًا إلى وحدة الجرائم الإلكترونية بوزارة الداخلية للإبلاغ عمّا حدث معك خاصّةً في حالة سرقة الأموال.	
3	في حال سرقة بيانات حساباتك البنكيّة أو البطاقات الائتمانيّة؛ تواصل مع البنك فورًا لوقف أيّ تعاملات على حسابك.	
4	عليك كتابة منشورات تشرح فيها كيف تَعرّضْت للتّصيُّد الاحتياليّ كيلا يقع غيرك في الفخّ نفسه.	
5	أوقِفْ جميع أنواع التّواصل مع هذا المُحتال الذي حاول أن يَخْدَعَك.	
6	في حالة كان التّصيُّد من خلال إعلان لوظيفة ما، عليك الإبلاغ فورًا عن الإعلان المشبوه.	
7	إن كنت تعتقد أنّ حاسوبك أو هاتفك تعرّض للخرق، فعليك أن تُوقِف اتّصاله بالإنترنت فورًا وأن تذهب لمتُخصّص لمساعدتك من أجل تأمين جهازك ووَضْع برامج للحماية.	

التَّمرين الخامس

ضَعْ علامَة (✅) أو علامة (❌) أمام العبارات التَّالية:



1. فتح أيّ رسائل نصّيَّة تَصِل على الهاتف حتى من الأرقام المجهولة.
2. فتح الرَّوابط والمُرفقات التي تأتي من خلال البريد الإلكترونيّ.
3. تقديم البيانات السِّرِّيَّة الخاصَّة بك عبر الهاتف، سواء للأسرة أم للجِهات المسؤولة.
4. مُشارَكة كثير من المعلومات الشَّخصيَّة عبر منصَّات التَّواصل الاجتماعيّ.
5. استخدام كلمات مرور قويَّة.

6 تجنُّب استخدام برامج الحماية والجدران النَّاريَّة.

7 إرسال الأموال إلى الجمعيَّات الخيريَّة التي تتواصل معك دون التَّأكُّد منها.

8 مُشارَكة بيانات بطاقاتك البنكيَّة على مواقع التَّسوُّق الإلكترونيّ كلّها.

9 تَجنَّب الإفصاح عن أيّ بيانات شخصيَّة أو معلومات حسَّاسة تخصُّك.

10 الرُّجوع إلى البنك قبل الإفصاح عن أيّ بيانات خاصَّة من المكالمات التي تَدَّعي أنَّها من خدمة عملاء البنوك.

انْتَبِه!

الهجوم الاحْتِيَالِيّ (Pharming)

كلمة Pharming هي عبارة عن مزيج من الكلمتين "Phishing" و"farming"، وهي عمليَّة احتيال عبر الإنترنت تُشبه التَّصيُّد الاحْتِيَاليّ؛ حيث يتمّ تصميم موقع ويب مُزيَّف، ثم إعادة توجيه المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ إليه لسرقة المعلومات السِّرِّيَّة.

التَّمرين السَّادس

عمليَّات الشِّراء الإلكترونيَّة.	
التَّسجيل في المواقع الإلكترونيَّة.	
تحميل التَّطبيقات من مَتاجِر التَّطبيقات.	
التَّحدُّث عبر الهاتف.	
التَّسجيل في النَّشرات العامَّة.	
الذَّهاب في نزهة.	
بيع وشراء الأسهم.	
الاشتراك في المجلَّات الإلكترونيَّة.	
فتح حساب بنكيّ.	
منشورات منصَّات التَّواصل الاجتماعيّ.	
مشاهدة برامج على التِّلفاز.	
مشاركة المعلومات والصُّور مع الأصدقاء.	
إعادة نَشْر المقالات والمعلومات التي تقرأها.	
الاشتراك في المَدوَّنات الصِّحِّيَّة.	
نَشْر المقاطع المُصَوَّرة عبر منصَّات التَّواصل الاجتماعيّ.	

انْتَبِه!

التَّصيُّد الخادع

(Deceptive Phishing)

يستخدم المُهاجِمُون الإلكترونيُّون تقنية خادعة للتَّظاهُر بأنَّهم يعملون مع شركة حقيقيَّة، لإبلاغ المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ بأنَّهم يَتعرَّضُون بالفعل لهجوم إلكترونيّ، لدَفْعهم للنَّقْر على رابطٍ مُعيَّن، لكنَّه في الحقيقة ضارٌّ، ما يتسبَّب في إصابة أجهزة الحاسوب الخاصَّة بهم.


ثانيًا: التَّمارين اللّاصَفّيّة

انْتَبِه!

التَّصيُّد الاحْتِيَاليّ المنبثق

(Pop-up Phishing)

يُقصَد به ظهور رسائل احْتِيَاليَّة للمُسْتَخْدِمِينَ في أثناء تصفُّحهم لشبكة الإنترنت؛ حيث يصيب المُهاجِمون مواقع الويب الأصليَّة ببرمجيات ضارَّة ما يتسبَّب في ظهور هذه الرَّسَائل المنبثقة عند زيارتها.

هل تعلم؟

تصيُّد التَّوأم الشِّرِّير: هو هجوم إلكترونيّ يعمل على خداع المُستهدَفين للاتِّصال بشبكة Wi-Fi مزيَّفة تُشبِه الأصليَّة.

انْتَبِه!

التَّصيُّد الاحْتِيَاليّ الموجَّه لكبار الشَّخصيّات

هو هجوم تَصيُّد احْتِيَاليّ يَستهدف كبار المسؤولين التَّنفيذيِّين في المُؤسَّسَات العالميَّة، ويأتي مُتنكِّرًا في صورة رسالة بريد إلكترونيّ مألوفة، وهو مُصمَّم على تحفيز ضحاياه على القيام بإجراءات مثل تحويل الأموال أو إرسال بيانات شخصيَّة.

أهداف هجمات التَّصيُّد الاحْتِيَاليّ الموجَّه لكبار الشَّخصيّات

1. دَفْع الضَّحايا للنَّقْر على روابط لمواقع تتضمَّن برمجيات ضارَّة.
2. طلب تحويل الأموال إلى الحساب المصرفيّ للمُهاجِم الإلكترونيّ.
3. طلب بيانات خاصَّة بالمُؤسَّسَات أو الأفراد لشَنّ المزيد من الهجمات مثل هجوم الفِدْيَة.

التَّمْرين الأوَّل

استخـرج الكلمـات التّالية من الجـدول:

توجيه

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

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

الاحتيال - ~~التَّصَيُّد~~ - جَريمَة - الرَّسائل - الفَخّ -الضَّحايا- البريد - الصَّوت - التَّلاعب - الخَوْف - بيانات - سرقة- سِرِّيَّة - كلمة مرور - هجوم

انْتَبِه!

استنساخ التَّصيُّد

(Clone Phishing)

يُقصَد به قيام أحد المُتَسَلِّلين بعمل نُسخة مُطابِقَة من الرِّسَالة التي استلمها المُستلِم بالفِعْل. وقد تتضمَّن شيئًا مثل عبارة "إعادة إرسال هذا"، مع وَضْع رابط ضارّ في البريد الإلكترونيّ.

التّمرين الثّاني

هل يمكنك تحديد إذا ما كانت الرّسالة التي وصلت على بريدك الإلكترونيّ حقيقيَّة أم مجرَّد تصيُّدٍ احتياليّ؟ وكيف ستتصرَّف حيالها؟

التّمرين الثّالث

هل تعرف أحدًا في محيطك -من العائلة أو الأصدقاء- سبق له أن تعرَّض لهجوم "التَّصَيُّد الاحتياليّ"؟ وكيف كان هذا الهجوم؟ وكيف تَصَرَّف حيال الأمر؟ وهل تعتقد أنّ تَصَرُّفه كان حكيمًا أم كان يجب أن يفعل شيئًا آخر؟

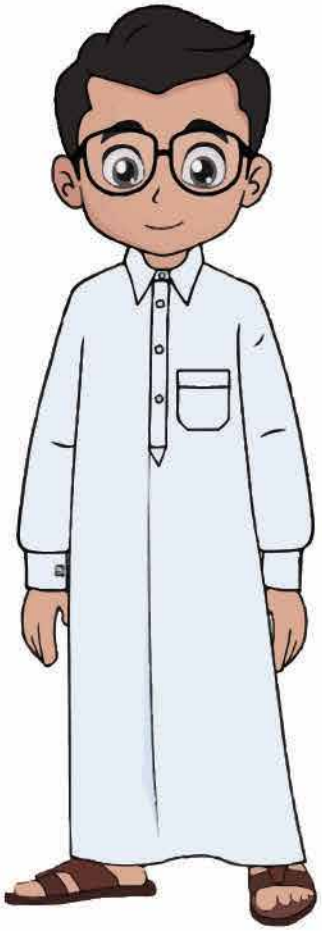

01001110
01110100
0111011101
111100010110

التّمرين الرّابع

ضَعْ علامة (✓) أو علامة (✗) أمام العبارات التّالية

تحقّق من المُرسِل، خاصّةً في أثناء فتح رسائل البريد الإلكترونيّ التي تحتوي على مُرفَقات.		
قُمْ بفتح أيّ رسالة بريد إلكترونيّ من أيّ شخص حتى لو لم تكن تعرفه.		
قَدّم بلاغًا لمزوّدي الخدمة حيال البريد الإلكترونيّ المَشْبوه.		
قُمْ بالرّدّ على أيّ مكالمات أو رسائل تَطْلُب بياناتك الشّخصيّة؛ حيث لا ضرر في ذلك.		
مرّر المؤشّر على الرّابط للتّأكُّد من أنّه موقع حقيقيّ قبل الدُّخول عليه.		
شارِك في العروض التّرويجيّة واترك بريدك الإلكترونيّ في كلّ المواقع والمنصّات.		
لا بأس في زيارة مواقع الإنترنت الغريبة أو ذات الامتدادات غير المعروفة.		
ابحث عن الأخطاء النّحويّة أو الإملائيّة؛ لأنّها مؤشّر مهمّ للرّسائل المزيّفة.		
في حالة التّعرُّض لهجوم أو خَرْق، لا تقلق، وإياك أن تُبلّغ الجهات المسؤولة.		
لا تَشْغَل بالك بتحديث الأنظمة أو التّطبيقات الموجودة على حاسوبك أو هاتفك.		

التَّمرين الخامس



قدِّم 5 نصائح لشخص ما سيستخدم شبكة الإنترنت للمرَّة الأولى وتريد أن تساعده وتحميه من الوقوع ضحيةً للتصيد الاحتيالي:

التَّمرين السَّادس

عَـــــرِّف المصطلحات التَّـــــالية

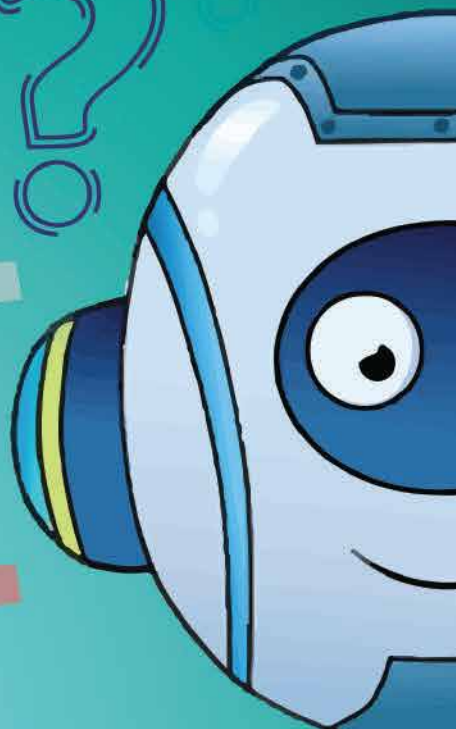
الهندسة الاجتماعيَّة .....

كلمة المرور .....

التَّصَيُّد الاحتياليّ .....

البَصْمة الرَّقميَّة .....

الاحتيال عبر الإنترنت .....



أهداف هجمات التَّصيُّد الاحْتِيَالِيّ

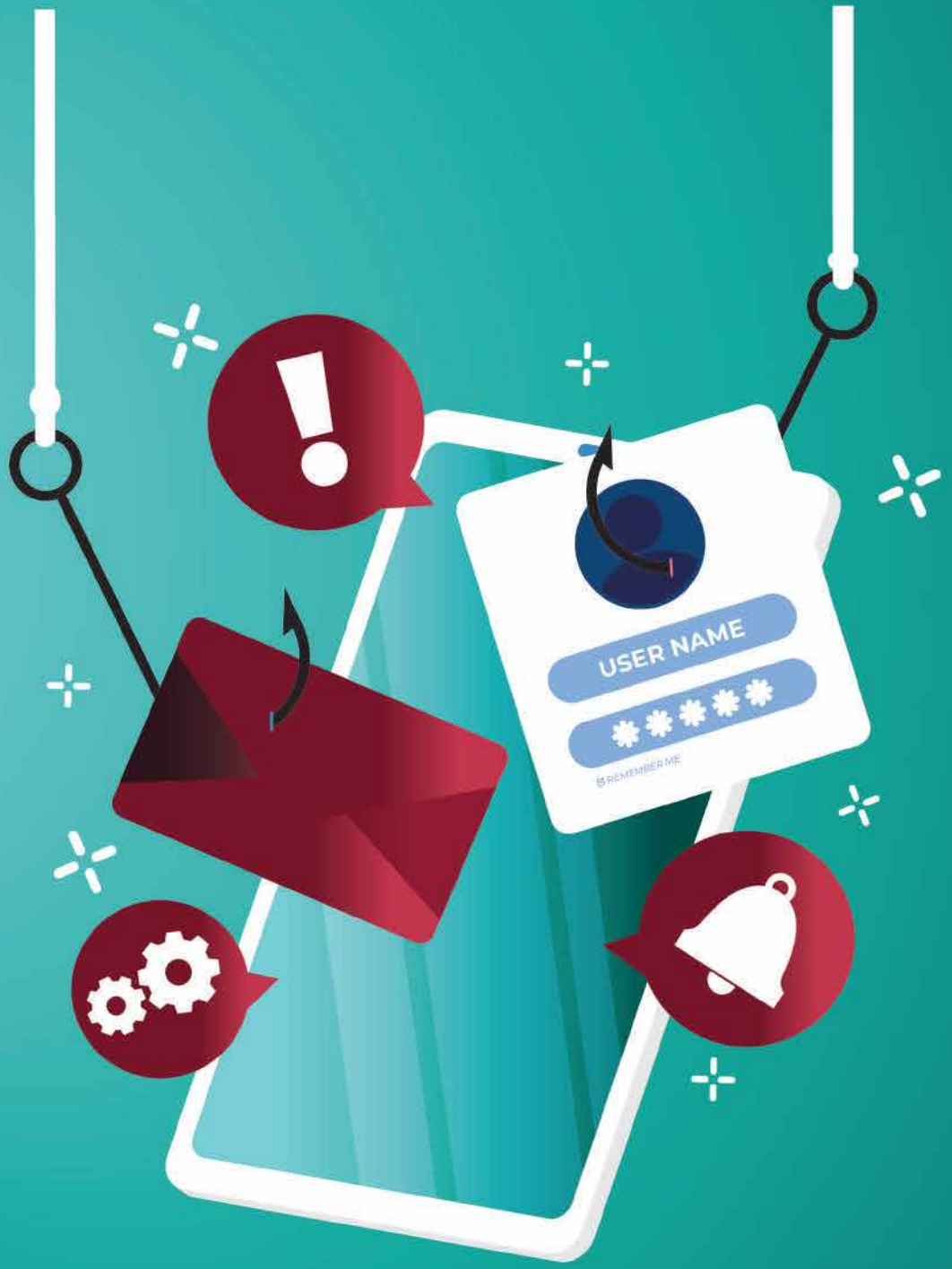
1. سرقة المعلومات أو الأموال من المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.
2. تثبيت البرمجيَّات الضَّارَّة على أجهزة المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.
3. تكون بوَّابة لتنفيذ عمليَّات أخرى لتخريب أنظمة المُؤسَّسَات المُسْتَهْدَفة.
4. دَفْع المُسْتَخْدِم الضَّحيَّة للدُّخُول إلى موقع مُزيَّف على الإنترنت لإكمال خطَّة الهجوم الاحْتِيَالِيّ.

علامات تُمَيِّز الرَّسَائل البريديَّة التَّصيُّديَّة

1. أسلوب الكتابة غير المألوف للمُستقْبِل.
2. الأخطاء النّحويَّة والإملائيَّة.
3. التَّناقُض في عناوين البريد الإلكترونيّ والرَّوابِط.
4. الإلحاح وإثارة مَشاعر الخوف.
5. المُرفَقَات المَشْبُوهَة.
6. طَلَب تحميل برامج وروابط.
7. رسائل الجوائز.
8. تزييف صفحات الويب.
9. استهداف المُوظَّفين في المُؤسَّسَات.

تصيُّد التَّوأم الشِّرير

هو هجوم إلكترونيّ يعمل على خداع المُسْتَهْدَفِينَ للاتِّصال بشبكة Wi-Fi مُزيَّفة تُشبه الأصليَّة، وعند الاتِّصال يبدأ المُهاجِم بالتَّسَلُّل إلى الأجهزة الخاصَّة بالضَّحايا لسرقة كلّ ما عليها من بيانات وملفَّات.



من علامات التَّمييز بين الرَّسَائل التَّصيُّديَّة وبين الرَّسَائل الحقيقيَّة المُرسَلة: أنَّها مَليئة بعبارات تُشْعِر المُسْتَخْدِم بالخَوْف والرَّغبة في اتِّخاذ قرار فَوريّ للتَّغلُّب على هذا الخوف والقلق الصَّادر عن محتواها.


أسئلة
المسابقات

ضَع المُسمّى المُناسِب

- هو هجوم عبر الإنترنت يعمل على خداع المُستهدَفين للاتّصال بشبكة Wi-Fi مزيّفة تُشبه الأصليّة، وعند الاتّصال يبدأ المُهاجِم التّسلُّل إلى الأجهزة الخاصّة بالضّحايا لسرقة كلّ ما عليها من بيانات وملفّات.

- هو هجوم احتياليّ يَستهدِف كبار المسؤولين التّنفيذيّين في المؤسّسات العالميّة، ويأتي متنكّرًا في صورة رسالة بريد إلكترونيّ مألوفة، وهو مصمّم على تحفيز ضحاياه على القيام بإجراءات مثل تحويل الأموال أو إرسال بيانات شخصيّة.

- هو هجوم احتياليّ يقوم فيه أحد المُتسلّلين بعمل نسخة مطابقة من الرّسالة التي استلمها المُستلِم بالفعل، وقد تتضمّن شيئًا مثل عبارة "إعادة إرسال هذا" ووَضْع رابط ضارّ في البريد الإلكترونيّ.

- هو هجوم احتياليّ يَستخدِم فيه المُهاجِم تقنيّة خادعة للتّظاهر بأنّه يعمل مع شركة حقيقيّة لإبلاغ المُستخدِمين المُستهدَفين بأنّهم يتعرّضون بالفعل لهجوم إلكترونيّ، لدفعهم للنّقر على رابط معيّن لكنّه في الحقيقة ضارٌّ؛ ما يتسبّب في إصابة أجهزة الحاسوب الخاصّة بهم.

- هجوم يتنكّر فيه المُهاجِمون الإلكترونيُّون في شخصيّة كيان معروف أو شخص حَسَن السُّمعة في رسالة بريد إلكترونيّ أو أيّ شَكْلٍ آخر من أشكال الاتّصال.

- هو هجوم احتياليّ يَسْتهدِف فردًا ما داخل مؤسّسة معيّنة؛ بغرض سرقة بيانات اعتماد تسجيل الدُّخول الخاصّة به.

- هو أحد أنواع هجمات التَّصَيُّد الاحتياليّ التي يتمّ تنفيذها عبر المكالمات الهاتفيّة؛ بغرض الحصول على أموال الضَّحايا أو المعلومات الشَّخصيّة الأخرى.

- هو هجوم احتياليّ يتمّ عن طريق إرسال رسالة بريد إلكترونيّ إلى المُستخدِم المُستهدَف، تتضمّن رابطًا إلى موقع ويب مزيّف، بهدف خداع الضَّحيّة لإدخال معلوماته الخاصّة.

- هو هجوم يتسبّب في ظهور رسائل احتياليّة للمُستخدِمين في أثناء تصفُّحهم شبكة الإنترنت؛ حيث يُصيب المُهاجِمون مواقع الويب الأصليّة ببرمجيّات ضارّة؛ ما يتسبّب في ظهور هذه الرّسائل المنبثقة عند زيارتها.

أكمل الجمل التَّالية

- يُعَدّ ..... إحدى الجَرَائم الإلكترونيَّة الأكثر انتشارًا في العالَم.

- في التَّصَيُّد الاحتياليّ يمكن استخدام الذَّكاء الاصطناعيّ في ابتكار ..... لاستغلاله عبر الهاتف للتَّحايل على الضَّحايا.

- يَصْعُب التَّمييز بين الرَّسائل التَّصَيُّديَّة وبين الرَّسائل الحقيقيَّة المُرسَلة للمستخدمين، لكن هناك علامة هي كثرة ..... بها.

- الهدف من هجمات التَّصَيُّد الاحتياليّ هو سرقة ..... أو ..... من المُستخدِمين المُستهدَفين، و..... على أجهزة المُستخدِمين، ودَفْع الضَّحِيَّة للدُّخول إلى ..... على الإنترنت.

- من طُرق المُهاجِمين الإلكترونيِّين لخَرْق أجهزة المُستخدِمين المُستهدَفين إرسال ..... تحتوي على ..... تتضمَّن ..... عند النَّقر عليها تسمح لـ ..... بالتَّسلّل إلى جهاز الحاسوب.

- من علامات تعرُّض الأجهزة الإلكترونيَّة للخرق تلقِّي إشعارات عبر البريد حول ..... رغم عدم قيام المُستخدِم بذلك، ..... الجهاز، وارتفاع ..... ، وتأخُّر الأوامر التي يتلقَّاها من المُستخدِم.

- يُمثِّل ظهور ..... تحتوي على رسائل مزعجة تدَّعي إصابة جهازك الإلكترونيّ بالفيروسات إحدى علامات تعرُّض الجهاز للخرق.

- من الأخطاء التي يرتكبها مستخدمو الإنترنت: التَّصفُّح على شبكة ..... ، وعدم تحديث ..... و ..... الموجودة على الأجهزة، إلى جانب مشاركة كثير من ..... على وسائل التَّواصل الاجتماعيّ.

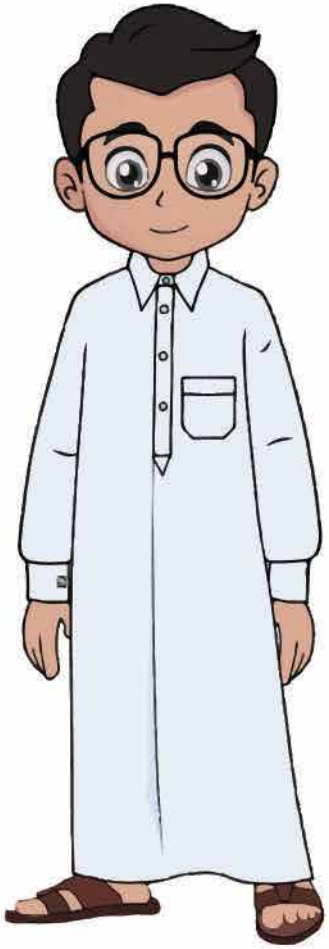
- ..... هي مسار البيانات التي يتركها المُستخدِم عند استخدام شبكة الإنترنت.

- من طُرق حماية البيانات من القرصنة: استخدام ..... ، فهي تُمثِّل خطّ الدِّفاع الأوَّل ضدّ الهجمات الاحتياليَّة.

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

١- من الأخطاء التي يقع فيها مُستخدِم الإنترنت خلال أداء مَهامّه أو التّصفُّح على الشبكة العالميّة:

- التّصفُّح على شبكة Wi-Fi العامّة دون اتّخاذ الاحتياطيات الأمنيّة. ◯
- تحديث المُتصفّح والتّطبيقات الموجودة على الأجهزة. ◯
- مُشارَكة الكثير من المعلومات الشّخصيّة على وسائل التّواصُل الاجْتِماعيّ. ◯
- اختلاف كلمات المرور لعددٍ من الحسابات الشّخصيّة للمُستخدِم عبر الإنترنت. ◯
- تثبيت تحديثات البرنامج تلقائيًّا. ◯
- فتح الرّوابط من رسائل البريد الإلكترونيّ دون التّحقُّق من موثوقيتها. ◯
- عدم الاستفادة من إعدادات الخصوصيّة الخاصّة بك على وسائل التّواصُل الاجْتِماعيّ. ◯



2- طرق تشكل البَصْمَة الرَّقميَّة:

- التَّسجيل في النَّشرات البريديَّة بالمواقع الإلكترونيّة والنشرات الإخباريَّة.
- تقييد النَّشر على وسائل التَّواصُل الاجْتِمَاعيّ.
- الابتعاد عن المعاملات الماليَّة عبر الإنترنت مثل التَّسوُّق.

3- الفرق بين التَّصيُّد الاحْتِيَاليّ والتَّصيُّد الاحْتِيَاليّ المُوجَّه:

- هجمات التَّصيُّد الاحْتِيَاليّ مُخصَّصة لهدف مُحدَّد، فهي هجمات شديدة الخصوصيَّة تَستهدف ضحيَّة بعَيْنها.
- تحتاج هجمات التَّصيُّد الاحتياليّ الموجَّه إلى مزيدٍ من الوقت والجُهْد لتنفيذها.
- هجمات التَّصيُّد الاحتياليّ الموجَّه هجمات واسعة النِّطاق تَستهدف البيانات الحسَّاسَة للمُسْتَخْدِمِينَ بشكلٍ عامّ.

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجبٌ تقوم به بمُفْرَدك أو بالاشتراك مع زميل أو زميلين من زملائك، تقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

- كتابة قِصَّة قصيرة تَدُور أحداثها حول طَالب تَعرَّض لحادثة تصيُّد احْتِيَاليّ، وكيف تَصرَّف حِيَال هذا الموقف.
- يَتَقَمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوجيهات عامَّة لزملائه أو أهْله يُوضِّح لهم فيها الإجراءات المطلوبة للوقاية من مَخاطِر الوُقُوع في حوادث تَصيُّد احْتِيَاليّ.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency