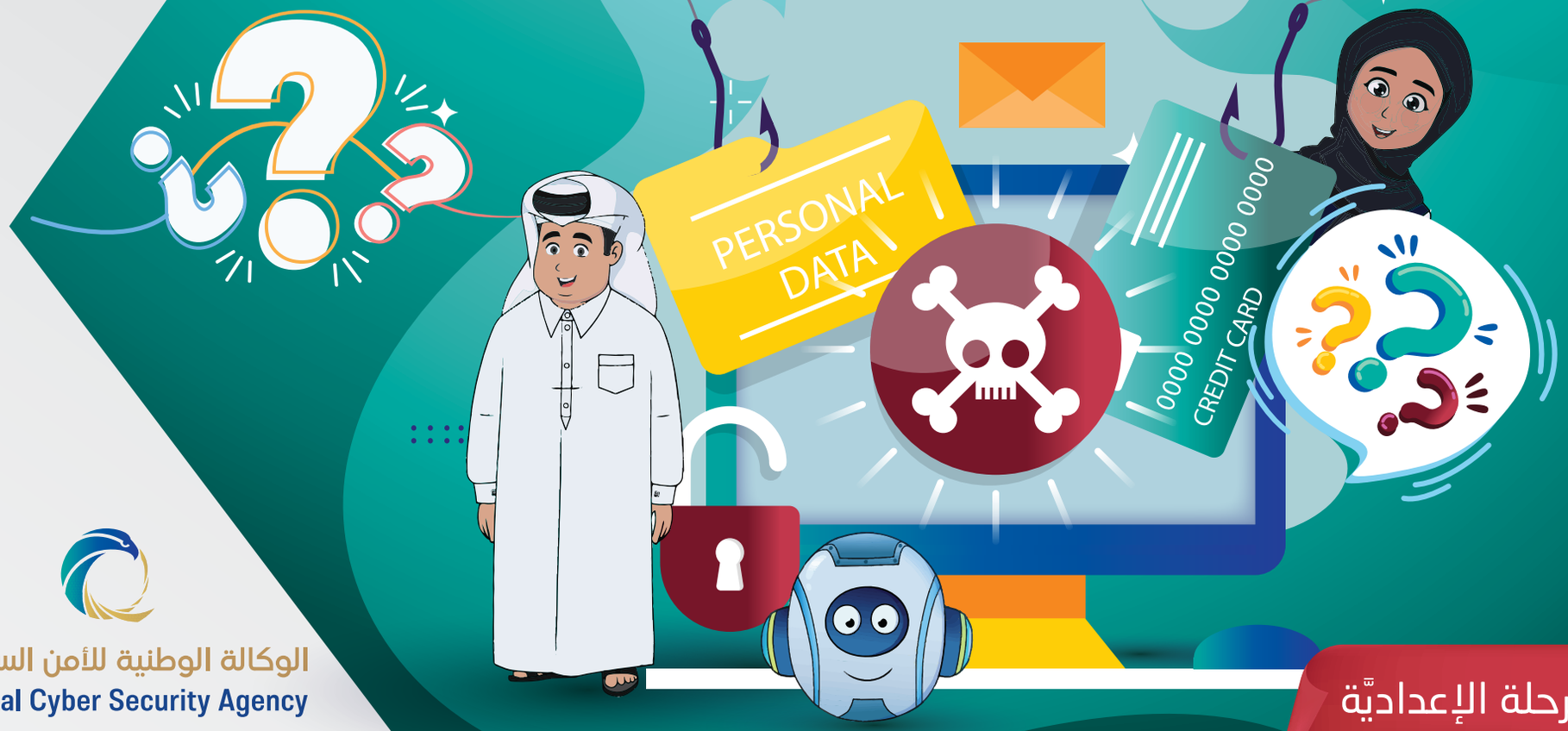
CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

هُجُوم التَّصيُّد الاحْتِيَالي

الحَقِيبَة التَّدريبيَّة

خاصَّة بالمُدَرِّب



المرحلة الإعداديَّة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

هجوم التَّصيُّد الاحتياليّ

المَرْحَلة الإعداديَّة

المادَّة التَّدريبيَّة

(حَقيبَة خاصَّة بالمُدَرِّب)

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

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

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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

المحتوى العام للحقيبة

أولاً: مدخل عام للحقيبة

ثانياً: المادة العلمية

أولًا: مَدْخل عامّ إلى الحَقيبَة التَّدْريبيَّة

فيما يلي تبيان لبعض التَّفاصيل ذات الصِّلَة المُباشِرَة بأهداف الحَقيبَة التَّدْريبيَّة، مع توجيهات عامَّة للمُدَرِّب حول كيفيَّة التَّعامُل مع هذه الحَقيبَة، وتزويده بالمحتوى العِلْميّ الذي سيَعْتَمِد عليه في التَّدريب.

الفكرة العامَّة

تقوم فِكْرة هذه الحَقيبَة التَّدريبيَّة على تزويد المُدَرِّب بأدوات ووسائل تدريبيَّة؛ بحيث يسهل عليه تقديم المعلومات للمُتَدَرِّبين. وبِشَكْلٍ عامّ، فإنَّ كُلّ مادَّة تدريبيَّة تكون على جُزْأين؛ جُزْء لدى المُتَدَرِّب وجُزْء آخر لدى المُدَرِّب، والحَقيبَة التَّدريبيَّة تُعدّ مُوجِّهًا عامًّا للمُدَرِّب وداعِمًا له، ومحتواها العِلْميّ هو ذاته لدى المُتَدَرِّب، ولكنْ بأسلوب عَرْضٍ مُخْتَلِفٍ؛ إضافةً إلى تزويد المُدَرِّب بأدواتٍ ووسائل تدريب تَدْعَمه في عمليَّة التَّدريب.

أهداف الحَقيبَة التَّدْريبيَّة

1. تَزويد المُدَرِّب بوسائل تدريب تُساعده على إيصال المحتوى التَّدريبيّ للطَّلَبة.
2. تَقديم المعلومات والمحتوى التَّدريبيّ بشكلٍ سَهْل ومُبسَّط.
3. تَقْديم المحتوى التَّدريبيّ الخاصّ بالتَّصيُّد الاحتياليّ مُرفَقًا بأدوات ووسائل تدريب مُتَعَدِّدَة.

محتوى الحَقيبَة التَّدْريبيَّة

تتضمَّن الحَقيبَة التَّدريبيَّة عدَّة أدوات تدريبيَّة، فيما يلي تبيان لها:

1. **ملفّ العَرْض.**
2. **ألعاب تدريبيَّة**، كالكلمات المُتَقاطِعَة والمُسابَقات، يعرضها المُدَرِّب على الطَّلَبة؛ بهدف ضمان تَفاعُلهم مع المحتوى التَّدريبيّ.
3. **فيديوهات تَعليميَّة.**
4. **مُسابَقات**، وهي على شَكْل أسئلة استنتاجيَّة يَعْرضها المُدَرِّب على الطَّلَبة بهدف التَّفاعُل فيما بينهم.
5. **بطاقات تدريبيَّة**، وهي على شَكْل معلومات عامَّة مُرفَقة بصُوَر تعبيريَّة، يَعْرضها المدرِّب على الطَّلَبة.
6. **إسكتشات**، تتضمَّن معلومات حول المَحاوِر الرَّئيسة في المُحتَوى التَّدريبيّ.

فِهْرِس المحتوى العِلْميّ للحَقيبَة التَّدريبيَّة

التَّوزيع الزَّمنيّ للوَرشَة

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

دليل إرشادي للمُدَرِّب

فيما يلي تبيان لبعض الإرشادات العامَّة للمُدَرِّب، والتي تتمحور حول كيفيَّة اسْتِخدام هذه الحَقيبَة.

1. المحتـوى العِلْمِـيّ للحَقيبَـة قـد يكـون يَفُـوق قُـدْرة الطَّلَبـة علـى الاستيعاب، خاصَّةً فيما يتعلَّق بالمصطلحات والمفاهيم العامَّة؛ لذلك لا بُدَّ للمُدَرِّب أن يُبسِّط هذه المفاهيم ويُقدِّمها بصورةٍ قابلة للفَهْم مِن قِبَل طَلَبة المَرْحَلة الإعداديَّة.
2. عرض المُدَرِّب شرائح العَرْض عند كُلّ نقطة يتحدَّث عنها، فمثلًا في أثناء حديثه عن مفهوم التَّصيُّد الاحتياليّ يعرض الشَّريحة الخاصَّة بمفهوم التَّصيُّد الاحتياليّ.
3. بعد الانتهاء من شرح الفَصْلين الأوَّل والثَّاني من المادَّة العِلْمِيَّة، يُعطِي المُدَرِّب للطَّلَبة اختبارًا بسيطًا وهو "ضع علامة (✔) أو علامة (✘) أمام كُلّ جُمْلَة".
4. في أثناء شرح الفَصْل الأَوَّل، يُوزِّع المُدَرِّب على الطَّلَبة الصُّوَر المُصمَّمة خِصِّيصًا لفِقْرة "هل تعلم أن..؟".
5. يَعرِض المُدَرِّب الجزء الخاص بـ "إسكتشات" في أثناء قيام الطَّلبة بحل التَّمارين والتَّدريبات.
6. في نهاية التَّدريب يعرض المُدَرِّب أسئلة المُسابَقات المذكورة في نهاية الملفّ.
7. في أثناء عَرْض المادَّة العِلْمِيَّة لكلّ فَصْل، يَسْتَقطع المُدَرِّب فترةً من الوقت المُخصَّص له لعَرْض عددٍ من الرَّوابِط ذات الصِّلَة بمضمون الفَصْل.
8. يعرض المُدَرِّب الفيديوهات -المذكورة في مِلَفّ مُنْفصِل- على الطَّلَبة في نهاية كُلّ فَصْلٍ، أو في المَوضِع الذي يراه مناسبًا.
9. يذكر أمثلةً عن حَوادِث تصيُّد احتياليّ حدثت خلال عَرْض المادَّة العِلْمِيَّة.
10. يُرجى فَتْح باب المُناقَشة مع الطَّلَبة في المَواضِع التي يراها المُدَرِّب مُناسِبة.
11. فيما يخصّ التَّمارين المُوجَّهة للطَّلَبة؛ سيتمّ إرفاق ملفّ التَّمارين في نهاية هذه الحَقيبَة، وهذه التَّمارين تُقسَّم لجُزْأين؛ جُزْء يُقدَّم للطَّلَبة خلال التَّدريب، وهو تمارين صَفِّيَّة، والجُزْء الآخر يُكلَّف الطَّلَبة بالإجابة عَنْه في المنزل، وهو تمارين لاصَفِّيَّة، وسوف نُوضِّح هذه الجزئيَّة في نهاية هذه الحَقيبَة.

مشروع التَّخرُّج

مشروع التَّخرُّج هو عملٌ يَقُوم به الطَّالب، ويهدف لتحقيق عدَّة أهداف، فيما يلي تبيان لأهمّها:

- التَّأكُّد من أنَّ الطَّالب قد استوعَب المعلومات والأفكار التي قَدَّمها المُدَرِّب له، وأنَّه بات قادرًا على الاستفادة منها في حياته اليَوْميَّة.
- ترسيخ المعلومات والأفكار التي قَدَّمها المُدَرِّب للطَّالب.
- المشروع بمثابة رَبْط للأفكار والمعلومات النَّظريَّة بالواقع العَمَليّ والتَّطبيقيّ.

وفيما يَتَعلَّق بآليَّة تكليف الطَّلَبة بالمشروع وكيفيَّة تنفيذه، يمكن تقديم التَّوجيهات التَّالية:

- يمكن أن يكون مشروع التَّخرُّج فَرْديًّا أو جَماعيًّا، وفي حال كان جَماعيًّا يجب ألَّا يَتجاوز عدد الطَّلَبة المُشْتَرِكين في مشروعٍ واحدٍ ثلاثة طلاب.
- اختيار موضوع المشروع يكون مِن قِبَل الطَّلبة، ويمكن للمُدرِّب تقديم بعض المُساعَدة أو الأفكار في هذا المجال.
- موضوع مشروع التَّخرُّج لا بُدّ أن يكون مُنسجِمًا مع المحتوى التَّدريبيّ الذي قَدَّمه المُدَرِّب للطَّلَبة.
- يمكن أن يكون مشروع التَّخرُّج ضِمْن أحد التَّصوُّرَات التَّالية، وهي تَصوُّرَات غير مُلْزِمَة، فيمكن للمُدَرِّب اختيار تَصوُّرَات أخرى يراها مُناسِبَة، وفيما يلي تبيان لبعض المُقْتَرَحَات:
  - كتابة قِصَّة قصيرة تَدُور أحداثها حول طَالبٍ تعرَّض لِحَادِثة تصيُّدٍ احتياليّ، وكيف تَصرَّف حِيَال هذا الموقف.
  - يَتَقَمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوْجِيهاتٍ عامَّةً لزملائه أو أَهْله يُوضِّح لهم فيها الإجراءات المطلوبة للوقاية من مَخاطِر الوقوع في حَوادِث تصيُّد احتياليّ.

ثانيًا: المادَّة العِلْمِيَّة

الفَصْل الأَوَّل

مفهوم التَّصيُّد الاحتياليّ

- أوَّلًا: مفهوم التَّصيُّد الاحتياليّ.
- ثانيًا: أشكال التَّصيُّد الاحتياليّ.

01

أولًا: مفهوم التَّصيُّد الاحتياليّ

يُعدّ التَّصيُّد الاحتياليّ أحد أنواع الجرائم الرَّقميَّة الأكثر انتشارًا، وفي هذا النَّوْع يتمّ استغلال شَبَكة الإنترنت لخداع الضَّحايا المُسْتَهدَفين لسَرِقة بياناتهم الشَّخصيَّة مِثْل كلمات المرور، وأرقام بطاقات الائتمان، وذلك من خلال طُرُق وأدوات عِدَّة، مِنها إنشاء موقع إلكترونيّ مُزيَّف لاستدراج الضَّحيَّة؛ ويتمّ إرسال الرَّابط عَبْر البريد الإلكترونيّ أو رسائل الماسنجر للضَّغط عليها ومِنْ ثَمَّ السَّماح للقَراصِنة دون عِلْم المُسْتَخدِم بالدُّخول غير المصرَّح به إلى حسابات وأجهزة الضَّحايا وتثبيت برمجيَّات خبيثة تساعدهم في سَرِقة البيانات.

ويعتمد المُهاجِمون على أساليب الضَّغط النَّفسيّ لإقناع الضَّحايا بالتَّصرُّف دون تفكيرٍ، عَبْر سرقة هُويَّة شخصيَّة مألوفة، ثمَّ خَلْق شعورٍ زائفٍ بالحاجة، مُسْتَغلِّين مشاعر مِثْل الخَوْف والقلق للحصول على ما يريدون. ففي هذه الحالة يميل الأشخاص إلى اتِّخاذ قراراتٍ سريعةٍ عند إعلامهم بأنهم مُعرَّضون لخسارة المال، أو أنَّ هناك مشكلة قانونيَّة قد تواجههم، أو أنَّهم لن يتمكَّنوا من الوُصُول إلى أحد الموارد المُهمَّة لهم فيما بعد، وهذا يتمّ عَبْر إرسال رسالة تطلب من المُسْتَخدِم "اتِّخاذ إجراءٍ فوريّ"، فهذه حيلة احتياليَّة من المُهاجِمين الإلكترونيِّين.

وبِشَكْلٍ عامّ يُقصَد بالتَّصيُّد الاحتياليّ تَنكُّر المُهاجِمين الرَّقميِّين في شخصيَّة كيانٍ معروفٍ -كإحدى الشَّركات المعروفة ذات السُّمْعة الجيِّدة، أو شخص حَسَن السُّمْعة- وإرسال رسالة بريد إلكترونيّ أو أيّ شكلٍ آخر من أشكال الاتِّصال، وعادةً ما يستخدم المُهاجِمون رسائل البريد الإلكترونيّ الاحتياليَّة لتوزيع الرَّوابِط أو المُرْفَقات الضَّارَّة التي من خلالها يحصل المُهاجِم على بياناتٍ حسَّاسةٍ تهمّ الضَّحيَّة مثل بيانات اعتماد تسجيل الدُّخول، أو أرقام الحسابات البنكيَّة، أو المعلومات الشَّخصيَّة الخاصَّة بالعائلة أو العمل أو غيرها[1].

ويُعدّ التَّصيُّد الاحتياليّ إحدى الجرائم السِّيبرانيَّة الأكثر انتشارًا في العالم، وذلك كَوْن مسألة خداع الأفراد للضَّغط على الرَّوابِط الضَّارَّة الواردة في رسائل البريد الإلكترونيّ الاحتياليَّة أمرًا يسهل فعله بدلًا من تنفيذ هجومٍ اختراقيّ لأمن الحواسيب؛ فوَفْق التَّقرير الصَّادر عن شركة Cisco

1. Phishing, Alexander S. Gillis, Technical Writer and Editor. On site: https://cutt.us/5jBhs

حول تهديدات الأمن السّيبرانيّ لعام 2021، كُشِفَ عن مسؤوليَّة التَّصيُّد الاحتياليّ عن 90% من الاختراقات الأمنيَّة للبيانات في العَالَم. وفي بحث لـ IBM عام 2022، تمّ ربط التَّصيُّد الاحتياليّ بـ 550 هجومًا سيبرانيًّا كلَّف خسائر قُدِّرت بـ 4,9 مليون دولار[1].

وفي هذا النَّوْع من الهَجْمات السّيبرانيَّة يسرق المُهاجِم هُويَّة شخصيَّة أخرى عَبْر البريد الإلكترونيّ، أو أيّ من وسائل التَّواصُل مِثْل "Messenger"، أو الرَّسائل النَّصِّيَّة لخدمة الرَّسائل القصيرة (SMS)، بِغَرْض الحُصُول على معلوماتٍ حسَّاسةٍ عن المُسْتَخدِم الضَّحيَّة، ومن أجل القيام بذلك يستخدم المُهاجِم مصادر مفتوحة للحصول على معلوماتٍ شخصيَّةٍ عن الضَّحيَّة المُسْتَهدَفة، ومن هذه المصادر وسائل التَّواصُل الاجتماعيّ مثل "Facebook" حيث تُسْتَخدَم هذه المعلومات فيما بعد عند صياغة رسالة بريد احتياليَّة للتَّحايُل على الضَّحيَّة ومِنْ ثَمَّ اختراق أَمْنه السّيبرانيّ.

يتلقَّى المُسْتَخدِم الضَّحيَّة في هذا النَّوْع من الهَجْمات رسالةً يبدو ظاهريًّا أنَّها تابعة لجهةٍ موثوقٍ بها مِثْل المُؤَسَّسات العَالَميَّة "Microsoft" أو "Google" أو غيرهما، وبِمُجرَّد نَقْر المُسْتَخدِم على الملفَّات المُرفَقة بالرِّسالة -وهو في الغالب رابط تَشعُّبيّ يربطه بموقع ويب ضارّ- يبدأ الهجوم من خلال تثبيت برمجيَّات ضارَّة على جهازه أو توجيهه إلى مَواقِع إنترنت مُزَيَّفة، لتبدأ عمليَّة جَمْع المعلومات الحسَّاسة، مِثْل كلمات المرور وأرقام البطاقات البنكيَّة أو غير ذلك.

وما يزيد من مِصْداقيَّة تلك الرَّسائل التَّصيُّديَّة هو استخدام المُهاجِمين لأدوات الذَّكاء الاصْطِناعيّ مِثْل روبوتات الدَّرْدشة للتَّغلُّب على الصِّيغة الرَّكيكة للرَّسائل؛ ولا يتوقَّف الأمر على روبوتات الدَّرْدشة، بل يمكن استخدام الذَّكاء الاصْطِناعيّ أيضًا في ابتكار صَوْتٍ ما لاستغلاله عَبْر الهاتف للتَّحايُل على الضَّحايا عَبْر إيهامهم بأنَّ صاحب الصَّوْت يتبع لأحد الجهات المُهمَّة التي يتعامل معها الضَّحيَّة أو يربطه بها مصلحةٍ ما لتبدأ عمليَّة الخِداع والحُصُول على المعلومات الشَّخصيَّة منه.

وبِشَكْلٍ عامّ يَصعُب التَّمييز بين الرَّسائل التَّصيُّديَّة وبين الرَّسائل الحقيقيَّة المُرسَلة للمُسْتَخدِمين، لكنَّ العلامة الأكثر تمييزًا للرَّسائل التَّصيُّديَّة هي كَثْرة الأخطاء الإملائيَّة والنَّحويَّة بها، فضلًا عن استخدام المُهاجِم السّيبرانيّ لعناوين بريد إلكترونيّ مغايرة للعناوين الأصليَّة للجهات التي ينتحل شخصيَّتها؛ وعند النَّظر في النَّمط المُسْتَخدَم في صياغة الرَّسائل التَّصيُّديَّة، نجد أنَّها مليئة بعباراتٍ تُشعِر المُسْتَخدِم بالخَوْف والرَّغبة في اتِّخاذ قرارٍ فَوْريّ؛ للتَّغلُّب على هذا الخَوْف والقلق الصَّادر عن محتواها.

1. What Is Phishing? On site: https://cutt.us/PbZ3Y

وإجمالًا.. فإنَّ الهدف من هَجْمات التَّصيُّد الاحتياليّ يَتمثَّل في النِّقاط التَّالية:

- سَرِقة المعلومات أو الأموال من المُسْتَخدِمين المُسْتَهدَفين.
- تكوين بوَّابة لتنفيذ عمليَّات أخرى لتخريب أنظمة المُؤَسَّسات المُستهدَفة.
- تثبيت البرمجيَّات الضَّارَّة على أجهزة المُسْتَخدِمين المُسْتَهدَفين.
- دَفْع المُسْتَخدِم الضَّحيَّة للدُّخول إلى موقعٍ مُزيَّفٍ عبر الإنترنت لإكمال خُطَّة الهجوم الاحتياليّ.

وبهذا نجد أن التَّصيُّد الاحتياليّ ينتج عن عددٍ من الأضرار على مستوى الأفراد والمُؤَسَّسات، وبالنِّسبة للمُؤَسَّسات يمكن أن تَتَسبَّب الهَجْمات التَّصيُّديَّة في تَعطُّل العمليَّات الدَّاخليَّة بالمُؤَسَّسة، ومِنْ ثَمَّ تحدث خسائر ماليَّة كبيرة، فضلًا عن الإضْرار بسُمْعة المُؤَسَّسة حيث تصبح بيانات العملاء بها مُعرَّضة لخطر السَّرِقة والتَّلاعُب بها؛ وهو ما يضع المُؤَسَّسات في مواجهة مع اللَّوائح التَّنفيذيَّة الهادفة لحماية البيانات داخل الدُّوَل.

أمَّا الأفراد فإنَّ هَجْمات التَّصيُّد الاحتياليّ تَتَسبَّب في سَرِقة بياناتهم البنكيَّة ومعلوماتهم الشَّخصيَّة وإعادة استغلالها ما يَتَسبَّب بِضَررٍ أكبر يصل إلى حدّ تشويه السُّمْعة وتلفيق الأكاذيب وسَرِقة الهُوِيَّة.

أنواع التَّصيُّد الاحتياليّ

- **التَّصيُّد الاحتيالي عَبْر البريد الإلكتروني:** يعتمد على تِقنيَّات مِثْل الارتباطات التَّشعُّبيَّة الزَّائفة للتَّحايل على مُسْتَلمي البريد الإلكترونيّ لسَرِقة بياناتهم الشَّخصيَّة، وغالبًا ما يَتنكَّر المُهاجِم في صورة مُزوِّد حساباتٍ كبيرٍ مثل مايكروسوفت وجوجل أو زميل في العمل أو الدِّراسَة.

- **التَّصيُّد الاحتيالي لتثبيت برمجيَّات الفِدية الضّارة:** يقوم المُهاجِمون بـ"دَسّ برمجيَّات ضارَّة مُتَخفِّية" في صورة مُرْفَق موثوق مثل سيرةٍ ذاتيَّةٍ أو كَشْف حساب بنكيّ في رسالة بريد إلكترونيّ، وبمُجَرَّد فتحها من قِبَل المُسْتَخدِم الضَّحيَّة يتعطَّل النِّظام بالكامل.

- **التَّصيُّد الاحتيالي المُوَجَّه:** في هذا النَّوْع من الهَجْمات يستهدف المُهاجِمون أشخاصًا بِعَيْنهم، وذلك من خلال استغلال المعلومات التي تمّ جمعها عَبْر البحث في وظائفهم وحياتهم الاجتماعيَّة التي يتشاركونها عَبْر وسائل التَّواصُل الاجتماعيّ.

- **التَّصيُّد المُوجَّه لكبار الشَّخصيَّات (تصيُّد الحِيتان):** يستهدف هذا الهجوم السِّيبرانيّ شخصيَّات مُهمَّة في المجتمعات مِثْل مشاهير الفنّ ورجال الأعمال والسِّياسيِّين؛ إذ يتمّ عمل بحثٍ مُتَعمِّقٍ حول ضحاياهم المُسْتَهدَفين لاستغلال اللَّحظة المُناسِبة لسَرِقة بياناتهم البنكيَّة والبيانات الشَّخصيَّة المُهمَّة.

- **التَّصيُّد الاحتيالي عَبْر الرَّسائل القصيرة:** يُرسِل المهاجِم رسائل نصِّيَّة مُتَخفِّية في صورة جهات اتِّصالٍ ذات ثقة من شركاتٍ يعرفها المُسْتَخدِم الضَّحيَّة مثل: أمازون،أو جوجل، وغيرهما.

- **التَّصيُّد الصَّوْتيّ:** يسرق المُهاجِمون الذين يسعون إلى خداع الأشخاص لإمدادهم ببياناتٍ حسَّاسة عَبْر الهاتف، هُوِيَّة شخصيَّات في وظائف مُعيَّنة تهمّ الضَّحيَّة.

ثانيًا: أشكال التَّصيُّد الاحتياليّ

غالبًا ما يحدث التَّصيُّد الاحتياليّ عَبْر عِدَّة أشكالٍ، فيما يلي تبيان لأهمّ هذه الأشكال:

- **التَّصيُّد الاحتياليّ المُوَجَّه**

يُقْصَد بالتَّصيُّد الاحتياليّ الموجَّه استهداف فردٍ ما داخل مُؤَسَّسة مُعيَّنة؛ بغرض سَرِقة بيانات اعتماد تسجيل الدُّخول الخاصَّة به؛ حيث يجمع المُهاجِم الإلكترونيّ المعلومات الشَّخصيَّة عن الفرد المُسْتَهدَف قبل بَدْء الاحتيال، مِثْل الاسم والمَنْصِب وتفاصيل الاتِّصال الخاصَّة به. ويُنفِّذ المُهاجِمون الإلكترونيُّون التَّصيُّد الاحتياليّ الموجَّه؛ بهدف سَرِقة الهُوِيَّة أو الاحتيال الماليّ، أو التَّلاعُب في أسعار الأسهم، أو التَّجسُّس، أو سَرِقة البيانات السِّريَّة من أجل إعادة بَيْعها للمُهتمِّين بها وغالبًا يكونون من المُنافِسين. ومن الأفراد المُسْتَهدَفين بهذا النَّوْع من التَّصيُّد الاحتياليّ، المديرون التَّنفيذيُّون في المُؤَسَّسات الذين قد يفتحون رسائل بريديَّة غير آمِنَة؛ ممَّا يُتيح للمجرمين خَرْق النِّظام العامّ للمُؤَسَّسة عَبْر جهاز المسؤولين.

الفَرْق بين التَّصيُّد الاحتياليّ والتَّصيُّد الاحتياليّ الموجَّه

الفَرْق هنا في أنَّ هَجْمات التَّصيُّد الاحتياليّ الموجَّه كما هو ظاهر من الاسم، فهي مُخصَّصة لهدفٍ مُحدَّدٍ. أمَّا هَجْمات التَّصيُّد الاحتياليّ فهي هَجْمات واسعة النِّطاق تستهدف البيانات الحسَّاسة للمُسْتَخدِمين بِشَكْلٍ عامّ. ففي هذا النَّوْع من الهَجْمات الاحتياليَّة تكون رسالة البريد الإلكترونيّ مُخادِعة، لكن ليست مُصمَّمة لتُناسِب أفرادًا بعَيْنهم، وهنا يعتمد المُهاجِم على الكَمّ وليس الكَيْف؛ بمعنى أنَّه يرسل الرَّسائل الاحتياليَّة إلى قائمة من العناوين البريديَّة لعلّ مجموعة منها تقع في الفَخّ.

هذا الأمر بِخِلاف التَّصيُّد الموجَّه، فهي هَجْمات شديدة الخصوصيَّة تستهدف ضحيَّة بِعَيْنها وتبدو الرَّسائل البريديَّة أكثر مِصْداقيَّة؛ لكَوْنها تحمل عناوين على صلة بالضَّحيَّة، وبالتَّالي هذا النَّوْع من الهَجْمات التَّصيُّديَّة يحتاج إلى مزيدٍ من الوقت والجُهْد[1].

1. What is spear phishing? Definition and risks. On site: https://cutt.us/riHDD

- **التَّصيُّد الصَّوْتيّ**

هو أحد أنواع هَجْمات التَّصيُّد الاحتياليّ الذي يتمّ تنفيذه عَبْر المكالمات الهاتفيَّة أو البريد الصَّوْتيّ، بهدف الحُصُول على أموال الضَّحايا أو المعلومات الشَّخصيَّة الأخرى؛ والسَّبب وراء انتشار هذه الهَجْمات السِّيبرانيَّة ما يُعرَف بـ"الهندسة الاجتماعيَّة" وهي تقنيَّة حديثة تعتمد على الغرائز البشريَّة الطَّبيعيَّة مِثْل الثِّقة أو الخَوْف، وغيرها من مشاعر يَستغلّها المُهاجِمون السِّيبرانيُّون للتَّأثير على الضَّحايا لدَفْعهم إلى اتِّخاذ قرارٍ مُعيَّنٍ يقود إلى تحقيق هدف المُهاجِم مِثْل سَرِقة المال أو المعلومات الحسَّاسة.

وغالبًا ما يتظاهر المُهاجِم الإلكترونيّ بأنَّه أحد الأفراد الذين يعرفهم الضَّحيَّة أو مسؤول في مَصْلَحةٍ تَعامَل معها الضَّحيَّة مثل الجِهات الحكوميَّة أو شركات التَّأمين أو البنوك، ليبدأ في استدراجه للحصول على المعلومات المُهمَّة منه لتنفيذ بقيَّة خُطَّة الاحتيال؛ كما يمكن تنفيذ التَّصيُّد الصَّوْتيّ من خلال اللَّعب على وَتَر الرَّغبة في تحقيق مكاسب ماديَّةٍ عند الضَّحيَّة مثل إغرائه بعُرُوض شرائيَّة هائلة بأسعارٍ رمزيَّةٍ، أو عَرْض مُسابَقة وهميَّة ذات عائد ماليّ كبير، وغيرها من حِيَل مُغرِية ينتهجها المُهاجِم السِّيبرانيّ.

لذلك يجب على المُسْتَخدِم التَّوقُّف عن إعلام الآخرين عَبْر الهاتف بمعلوماته المُهمَّة؛ لأنَّ المُتَّصل في حالة كان من البنك لن يطلب معلومات شخصيَّة مثل أرقام البطاقات الائتمانيَّة عبر الهاتف، كما ينبغي التَّحقُّق من الرَّقم المُتَّصل بك أوَّلًا قبل الرَّدّ عليه، ويُفضَّل الاتِّصال به من رقم آخر؛ للتَّأكُّد من مِصْداقيَّته.

ولا يُفضَّل الرَّدّ على رسائل البريد الإلكترونيّ أو الرَّسائل النَّصِّيَّة أو رسائل وسائل التَّواصُل الاجتماعيّ التي تطلب معلوماتٍ شخصيَّةً مثل رقم الهاتف الخاصّ بك، ففي الغالب هي خُطْوة استباقيَّة قبل تَلقِّي مكالمة تَصيُّد صوتيَّة فيما بعد[1].

1. Vishing – a growing threat. On site: https://cutt.us/q3aSU

- **التَّصيُّد عَبْر البريد الإلكترونيّ**

فـي هـذا النَّـوْع مـن عمليَّـات التَّصيُّـد الاحتيالـيّ، يعتمـد المُهاجِـم السِّـيبرانيّ علـى البريـد الإلكترونـيّ لتنفيـذ هجومـه علـى الضَّحيَّـة؛ حيـث يرسـل رسـالةً بريديَّـةً تبـدو كأنَّهـا مـن مصـدرٍ موثـوقٍ بـه؛ بهـدف التَّسلُّل إلـى الجهـاز لسَـرِقة البيانـات الحسَّاسـة أو سَـرِقة المـال أو سَـرِقة الهُوِيَّـة واسـتغلالها فيمـا بعـد فـي جرائـم أخـرى مثـل هجـوم الفِدْيـة.

وهناك عِدَّة علامات لتمييز الرَّسائل البريديَّة التَّصيُّديَّة:

1. أُسْلوب الكتابة

مـن العلامـات المَبْدئيَّـة التـي يمكـن أن تكشـف الرَّسـائل التَّصيُّديَّـة هـي أُسْـلوب الكتابـة غيـر المألـوف للمُسْـتقبِل، فمثـلًا إذا حملـت الرِّسـالة اسـم شـخصيَّة قريبـة مـن الضَّحيَّـة، فمـن المُسْـتبعد أن يتـمّ التَّحـدُّث بصيغـةٍ رسـميَّةٍ، وهنـا إذا كانـت الرِّسـالة بهـذا الأُسْـلوب تتزايـد احتماليَّـة أن تكـون رسـالةً احتياليَّـةً.

2. الأخطاء النَّحويَّة والإملائيَّة

الأخطـاء الإملائيَّـة والنَّحويَّـة مـن العلامـات المُمَيِّـزة للرَّسـائل الاحتياليَّـة أيضًـا، فـإذا كانـت الرِّسـالة تَدَّعـي أنَّهـا مـن مُؤَسَّسـةٍ معروفـةٍ، مثـل جوجـل، فـإنَّ أغلـب المُؤَسَّسـات الكبـرى تمتلـك ميـزة التَّدقيـق الإملائـيّ والنَّحـويّ لرسـائلها البريديَّـة وهـو مـا يُميِّـز رسـائلها عـن غيرهـا.

3. التَّناقض في عناوين البريد الإلكترونيّ والرَّوابِط

يُعدّ البحـث عـن التَّناقـض فـي عناويـن البريـد الإلكترونـيّ والرَّوابِـط مـن إحـدى وسـائل كَشْـف الرَّسـائل الاحتياليَّـة، فمثـلًا علـى المُسْـتَخدِم مُطابَقـة عنـوان البريـد الإلكترونـيّ الـوارد مـن مُؤَسَّسـة كبيـرة مثـل جوجـل مـع العُنْـوان الأصلـيّ المُعْلَـن فـي موقعهـا الرَّسـميّ.

4. الإلْحاح وإثارة مَشاعِر الخَوْف

غالبًـا يلجـأ المُهاجِمـون الإلكترونيُّـون إلـى التَّلاعُـب بمشـاعر الضَّحايـا عَبْـر إثـارة الخَـوْف والقلـق لديهـم حيـال تعاملاتهـم البنكيَّـة أو معلوماتهـم الشَّـخصيَّة ويبـدؤون فـي طلـب بياناتٍ حسَّاسةٍ منهـم، وهُنَـا يجـب التَّيقُّظ لهذه المسألة وعـدم الوقـوع تحـت وَطْأة الضَّغـط المُمَـارَس والتَّمهُّـل للتَّفكيـر قبـل اتِّخـاذ أيّ إجـراء.

5. المُرْفَقات المشبوهة

فـي حالـة تَسـلُّم بريـد إلكترونـيّ يَتَضمَّـن مُرْفَقـات مـن مصـادر مجهولـة، يجـب الحـذر قبـل الضَّغـط عليهـا، والبحـث عـن المصـدر فـي مُحـرِّكات البحـث للتَّأكُّـد مـن وجـوده، ويحمـل هـذا النَّـوْع مـن المُرْفَقـات الضَّـارَّة

امتـدادات مثـل zip، exe، scr وغيرهـا مـن امتـدادات غيـر مألوفـة، لـذا يجـب فَحْـص المُرْفَقـات قَبْـل فتحهـا بواسـطة برمجيّـات الفيروسـات[1].

6. طَلَب تحميل بَرامِج ورَوابِط

إذا كانـت رسـالة البريـد الإلكترونـيّ تدَّعـي أنَّهـا مـن جهـةٍ مـا معروفـة، وتطلـب تثبيـت بَرامِـج مُعيَّنـة أو رَوابِـط علـى الأجهـزة، يجـب التَّيقُّـظ؛ ففـي الأغلـب تكـون رسـائل احتياليَّـة ويجـب عـدم الاسـتجابة لهـذه الأوامـر.

7. المُسْتَهدَف لم يبدأ المُحادَثة

فـي أغلـب عمليّـات الاحتيـال يتسـلَّم الضَّحيَّـة رسـالةً بريديَّـةً تدفعـه إلـى الـرَّدّ لتَلَقِّـي جوائـز ماليَّـة كبيـرة أو هدايـا عَيْنيَّـة ذات وقـت مُحـدَّد يجـب اللِّحـاق بـه، رغـم عـدم اشـتراكه فـي أيّ مُسـابَقة مـن قبـل؛ ممَّـا يعنـي أنَّ هـذا النَّـوْع مـن الرَّسـائل احتيالـيّ.

8. تزييف صفحات الويب

قـد يقـوم المُهاجِـم بإنشـاء صفحـةٍ مُزيَّفـةٍ ثـمَّ توجيـه رابـط منهـا إلـى الضَّحايـا للظُّهـور بمظهـرٍ رسـميّ موثـوقٍ بـه، لدَفْعـه إلـى إجـراءٍ مـا، مِثْـل: زيـارة الصَّفْحـة والتَّسـجيل فيهـا أو الضَّغـط علـى رابطهـا للوقـوع فـي الفَـخّ.

9. استهداف المُوَظَّفين في المُؤَسَّسات

قـد يتلقَّـى المُوَظَّفـون فـي المُؤَسَّسـات رسـائل بريديَّـة تصيُّديَّـة بهـدف إلْحـاق الضَّـرر بالمُؤَسَّسـة أو الدُّخـول إلـى نظامهـا، والتَّلاعُـب وسَـرِقة بيانـات العمـلاء واسـتغلالها أو بَيْعهـا لجهـاتٍ أخـرى خارجيَّـة. لـذا يجـب توعيـة المُوَظَّفيـن بأهمِّيَّـة الأمـن السِّـيبرانيّ، وتَجنُّـب الضَّغـط علـى رَوابِـط مجهولـة أو الـرَّدّ علـى رسـائل مـن جهـاتٍ غيـر مألوفـةٍ.

1. 10 Most Common Signs of a Phishing Email. On site: https://cutt.us/MJiQZ

- **التَّصيُّد الاحتياليّ عَبْر HTTPS**

يتـمّ تنفيـذ هجـوم التَّصيُّـد الاحتيالـيّ عَبْـر HTTPS عـن طريـق إرسـال رسـالة بريـد إلكترونـيّ إلـى المُسْـتَخدِم المُسْـتَهدَف تَتَضمَّـن رابطًـا إلـى موقـع ويـب مُزيَّـف، بهـدف خـداع الضَّحيَّـة لإدخـال معلوماتـه الخاصَّـة؛ وتُعـدّ مَواقِـع HTTPS الاحتياليَّـة المَنْفَـذ المُفَضَّـل للمُهاجِمين الذيـن لديهـم القُـدْرة علـى إيهـام الضَّحايا بأنَّهم مصدر موثوق به. وهـذا النَّـوْع مـن الهَجْمات الاحتياليَّـة يُوصَـف بأنَّـه مُنْخَفِـض المَخاطِـر ومُرْتَفِـع المَكاسِـب.

ومـن المُلاحَـظ أنَّ 91% مـن جميـع الهَجْمـات الإلكترونيَّـة تبـدأ برسـالة بريـد إلكترونـيّ تصيُّديَّـة يتـمّ إرسـالها إلـى ضحايـا غيـر مُتَوقّعيـن، وجَذْبهـم إلـى المَواقِـع عَبْـر رابـطٍ فـي الرِّسـالة المُرسَـلة مـن عنـوان شـرعيّ، مِثْـل شـركة معلومـة أو شـخص معـروف؛ وأكثـر الأمثلـة انتشـارًا لهـذا النَّـوْع مـن الهَجْمـات الاحتياليَّـة هـي شـركة Sony Pictures التـي تعرَّضـت فـي عـام 2014 لهجـومٍ عَبْـر رسـائل بريـد مُزَيَّفـة تَمكَّـن عبرهـا المُهاجِمـون مـن التَّسـلُّل إلـى الشَّـركة وسَـرِقة كلمـات المـرور وبيانـات مُهمَّـة منهـا نتيجـة ضغـط المُوظَّفيـن علـى رَوابِـط مُزَيَّفـة أُرْسِـلت إليهـم عَبْـر البريـد الإلكترونـيّ[1].

- **الهجوم الاحتياليّ المعروف بـ Pharming**

Pharming هـي عبـارة عـن مزيـج مـن الكلمتَيْـن "Phishing" و"farming"، وهـي عمليَّـة احتيالٍ عَبْـر الإنترنـت تُشبه التَّصيُّـد الاحتيالـيّ؛ حيـث يتـمّ تصميـم موقـع ويـب مُزَيَّـف ثـم إعـادة توجيـه المُسْـتَخدِمين المُسْـتَهدَفين إليـه لسَـرِقة المعلومـات السِّـرِّيَّة؛ وتهـدف هـذه المَواقِـع المُزَيَّفـة إلـى جَمْـع المعلومـات الشَّخصيَّة عـن الضَّحيَّـة، مِثْـل كلمـات المـرور وأرقـام الحسـابات البنكيَّـة، وغيرها. أو تحـاول تثبيـت برمجيَّـات ضـارَّة علـى أجهـزة الحاسـوب الخاصَّـة بالضَّحايـا، خاصَّـةً أولئـك العامليـن فـي القطـاع المالـيّ مِثْـل البنـوك أو مَواقِـع التِّجـارة عَبْـر الإنترنـت، بغـرض سَـرِقة الهُوِيَّـة؛ **ويُنَفِّـذ المُهاجِـم الإلكترونـيّ عمليَّتـه الاحتياليَّـة مـن خـلال أُسْـلوبين هُمَـا:**

- إرسـال تعليمـات برمجيَّـة ضـارَّة فـي رسـالة بريـد إلكترونـيّ بِغَـرَض تثبيـت فيـروس أو حصـان طـروادة علـى حاسـوب المُسْـتَخدِم المُسْـتَهدَف؛ حيـث تعمـل هـذه التَّعليمـات البرمجيَّـة الضَّـارَّة علـى توجيـه حركـة المـرور نحـو موقـع ويـب مُزَيَّـف حتَّـى لـو كتـب المُسْـتَخدِم عنـوان المَوْقِـع الإلكترونـيّ الصَّحيـح، فـإنَّ الهـدف مـن هـذه البرمجيَّـات الضَّـارَّة هـو تحويلـه إلـى المَوْقِـع المُزَيَّـف دون أن يعـي ذلـك.

1. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://cutt.us/20AV8

- يقوم المهاجم بواسطة تقنيَّة يُطلَق عليها "تسميم نظام أسماء النِّطاقات" بإجراء تعديلات في "نظام اسم المجال" (DNS) بهدف تحويل المُسْتَخدِم المُسْتَهدَف إلى مَواقِع الويب المُزَيَّفة بدلًا من المَواقِع الصَّحيحة دون قصدٍ منه، ليبدأ بعدها المُهاجِم في تثبيت الفيروسات أو أحصنة طروادة على حاسوب المُسْتَخدِم أو جَمْع معلوماتٍ شخصيَّة وماليَّة لاستخدامها في سَرِقة الهُوِيَّة[1].

وبعد الحُصُول على البيانات الشَّخصيَّة، يستخدمها المُهاجِمون إما في أهدافٍ احتياليَّةٍ أخرى أو بَيْعها إلى مُهاجِمين آخرين.

- **التَّصيُّد الاحتياليّ المُنْبَثِق Pop-up Phishing**

يُقصَد به ظهور رسائل احتياليَّة للمُسْتَخدِمين أثناء تصفُّحهم لشبكة الإنترنت؛ حيث يصيب المُهاجِمون مَواقِع الويب الأصليَّة ببرمجيَّات ضارَّة ممَّا يَتَسبَّب في ظهور هذه الرَّسائل المُنْبَثِقة عند زيارتها؛ وما يزيد من خطورة هذا النَّوْع من الرَّسائل التَّصيُّديَّة هو مُحْتَواها المُطَمْئِن للمُسْتَخدِمين؛ حيث تقدم تحذيرًا من الاحتيال لزوَّار هذه المَواقِع حول أمان أجهزتهم الإلكترونيَّة وتُطالِب الزَّائر بتنزيل بعض البرامج لإصلاح المشكلة، مثل مكافحة الفيروسات، إلَّا أنَّها في الحقيقة برمجيَّات ضارَّة هدفها التَّسلُّل إلى أجهزة زُوَّار مَواقِع الويب والاحتيال على مَالِكي الأجهزة.

وتَجنُّبًا لهَجْمات التَّصيُّد الاحتياليّ المُنْبَثِقة يُنصَح باتِّباع الآتي:

- في حال ظهور رسائل منبثقة على بعض المواقع الإلكترونيَّة التي تزورها، لا يعني بالضَّرورة أنَّ جهازك مصاب بالبرمجيَّات الضَّارَّة، فقد تكون البرمجيَّات الضَّارة موجودة على الموقع الذي تتصفحه، وفي حال تثبيتك برنامج مكافحة للبرمجيَّات الضَّارَّة لن تنتقل هذه البرمجيَّات إلى جهازك.
- ينبغي عدم مَنْح أيّ شخصٍ إمكانيَّة الوصول عن بُعْد إلى جهاز الحاسوب الخاصّ بك.
- في حالة الشَّكّ بمدى مِصْداقيَّة الرَّسائل التي تراها عليك التَّواصُل مُباشَرةً مع مالك المَوْقِع أو فريق الدَّعم الخاصّ به[2].

1. What Is Pharming and How to Protect Yourself. On site: https://cutt.us/BGtUl
2. Scam Alert: What You Need to Know About Pop-Up Phishing. On site: https://cutt.us/3pHtA

- **تصيُّد التَّوْأم الشِّرير**

هو هجوم سيبرانيّ يعمل على خِداع المُسْتَهدَفين للاتِّصال بِشَبَكة Wi-Fi مُزَيَّفة تشبه الأصليَّة، وعند الاتِّصال يبدأ المُهاجِم بالتَّسلُّل إلى الأجهزة الخاصَّة بالضَّحايا لسَرِقة كُلّ ما عليها من بياناتٍ وملفّاتٍ. **ويستخدم المُهاجِم عِدَّة خطوات لتنفيذ هجومه السِّيبرانيّ؛ فيما يلي تبيان لأهمّها:**

- اختيار مكان عامّ يَتَضمَّن خِدْمة Wi-Fi مجَّانيَّة، مِثْل المطارات والمكتبات العامَّة أو المقاهي، لبَدْء الهجوم.
- إعداد نقطة وصول Wi-Fi: يقوم المُهاجِم بإنشاء نقطة اتِّصالٍ جديدةٍ باستخدام اسم مألوف لتسهيل مُهمَّة جذب المُسْتَخدِمين للشَّبَكة والبَدْء في استخدامها.
- إنشاء صَفْحة بوَّابة مُقيَّدة مُزَيَّفة: يضع المُهاجِم بوَّابة على شَبَكة Wi-Fi العامَّة والتي تطلب من المُسْتَخدِمين كلمات مرور أو معلوماتٍ شخصيَّة للمرور إلى الشَّبَكة.
- الاقتراب من الضَّحايا: بعد انتهاء المُهاجِم من الخُطُوات السَّابقة يبدأ في توجيه أجهزته بالقُرْب من الضَّحايا المُحْتَمِلين لإنشاء إشارةٍ أقوى، وبالتَّالي يختارون الشَّبكة المُزَيَّفة لاستخدامها ممَّا يُؤدِّي إلى وقوعهم في الفَخّ.
- مُراقَبة وسَرِقة بيانات المُسْتَخدِم: بعد دخول المُسْتَخدِم المُسْتَهدَف للشَّبَكة يبدأ المُهاجِم بمُراقَبة ما يقوم به عَبْر الإنترنت ويجمع البيانات مِن أرقام ومعلومات مُهمَّة[1].

1. What is an Evil Twin Attack? On site: https://cutt.us/jsBji

- **التَّصيُّد الموجَّه لكبار الشَّخصيَّات**

هـو هجـوم تصيُّـد احتيالـيّ يسـتهدف كبـار المسـؤولين التَّنفيذيِّيـن فـي المُؤَسَّسات العَالَميَّة، ويأتـي مُتَنكِّرًا فـي صورة رسالة بريد إلكترونـيّ مألوفة، وهـو مُصَمّـم علـى تحفيـز ضحاياه للقيـام بإجـراءاتٍ مثـل تحويـل الأمـوال أو إرسـال بيانـاتٍ شـخصيَّةٍ؛ وتُعـدّ المُؤَسَّسـات الماليَّـة وخِدْمـات الدَّفـع هـي الأكثـر اسـتهدافًا مـن هـذا النَّـوْع مـن هَجْمـات التَّصيُّـد الاحتيالـيّ، إذ تحتـوي علـى معلومـاتٍ شخصيَّةٍ حـول المُؤَسَّسـات أو الأفـراد النَّافذيـن المُسْتَهدَفين؛ **ويهـدف هـذا النَّـوْع مـن الهَجْمـات لتحقيـق الأهـداف التَّاليـة:**

- دَفْع الضَّحايا للنَّقر على رَوابِط لمَواقِع تَتَضمَّن برمجيَّات ضارَّة.
- طلب تحويل الأموال إلى الحساب المَصْرِفيّ للمُهاجِم السّيبرانيّ.
- طلـب بيانـات خاصَّـة بالمُؤَسَّسـات أو الأفـراد لِشَـنّ المزيـد مـن الهَجْمـات مثـل هجـوم الفِدْيـة.

وإجمـالًا، فـإنَّ الأضـرار النَّاتجـة عـن التَّصيُّـد الموجَّـه لكبـار الشَّخصيَّات تشـمل الجوانـب التَّالية:

- **فُقْدان البيانات**

بِمُجـرَّد الضَّغـط علـى الرَّوابِـط أو تنزيـل مُرْفَقـات البريـد تبـدأ الشَّـبَكات الدَّاخليَّـة بالإصابـة بالبرمجيَّـات الضَّـارَّة التـي تُمكِّـن المُتَسـلِّلين مـن الدُّخـول وسَـرِقة مـا يرغبـون فيـه مـن بيانـاتٍ.

- **تَضرُّر سُمْعة المُؤَسَّسات والأفراد**

قـد يُـؤدِّي فُقْـدان البيانـات إلـى إلْحـاق خسـائر ماليَّـة كبيـرة بالمُؤَسَّسـات والأفـراد، فضـلًا عـن تَضـرُّر سُـمْعتها أمـام الجهـات الرَّسـميَّة فـي الدَّولـة التـي سـنَّت تشـريعاتٍ لحمايـة البيانـات.

وهـذه الهَجْمـات التَّصيُّديَّـة زادت صعوبـة كَشْـفها فـي الآونـة الأخيـرة؛ بسـبب اعتمـاد العناويـن البريديَّـة المُزَيَّفـة التـي تظهـر كأصليَّـة، بخـلاف المُصْطَلحـات التِّجاريَّـة والدَّمْـج بيـن العديـد مـن الأساليـب الاحتياليَّـة التي يفشـل المسـؤولون التَّنفيذيـون فـي كَشْـفها، وبالتَّالـي يقعـون ضحايـا لهجمـات التَّصيُّـد الموجَّـه لكبـار الشَّـخصيَّات، كمـا يمكـن لهَجْمـات صَيْـد الحيتـان اسـتخدام البريـد الإلكترونـيّ مـع المكالمـات الهاتفيَّـة لدَفْـع الضَّحيَّـة المُسْـتَهدَفة إلـى الاقتنـاع بالطَّلـب المُرسَـل عَبْـر البريـد، وبالتَّالـي فهـو هجـوم مُـزْدَوج، وتُعـدّ وسـائل التَّواصُـل الاجتماعـيّ أيضًـا وسـيلةً شـائعةً لتنفيـذ هَجْمـات التَّصيُّـد؛ حيـث تُوفِّـر معلومـات مهنيَّـة وشـخصيَّة عـن الأشـخاص المُسْـتَهدَفين[1].

1. Whaling: how it works, and what your organization can do about it. On site: https://cutt.us/H9RNo

- **استنساخ التَّصيُّد Clone Phishing**

يُقصَد به قيام أحد المُتَسلِّلين بعمل نُسْخةٍ مُطابِقةٍ من الرِّسالة التي تسلَّمها المُسْتَهدَف بالفعل. وقد تَتَضمَّن شيئًا مِثْل عبارة "إعادة إرسال هذا"، مع وَضْع رابط ضارّ في البريد الإلكترونيّ[1].

- **التَّصيُّد الخَادِع Deceptive Phishing**

يستخدم المُهاجِمون الإلكترونيُّون تقنيَّةً خَادِعةً للتَّظاهر بأنَّهم يعملون مع شركةٍ حقيقيَّة مِثْل شركة أبل Apple لإبلاغ المُسْتَخدِمين المُسْتَهدَفين بأنَّهم يتعرَّضون بالفعل لهجومٍ إلكترونيّ، لدفعهم إلى النَّقر على رابط مُعيَّن، لكنَّه في الحقيقة ضارّ؛ ممَّا يَتَسبَّب في إصابة أجهزة الحاسوب الخاصَّة بهم.

1. How Does Clone Phishing Work? On site: https://cutt.us/x7Gwg

الفَصْل الثَّاني

كيفيَّة تنفيذ هَجْمات التَّصيُّد الاحتياليّ

- أوَّلًا: الثَّغَرات التي يَستغلّها مُنَفِّذُو هَجْمات التَّصيُّد الاحتياليّ.
- ثانيًا: الأخطاء التي يرتكبها مُسْتَخْدِمُو الإنترنت.
- ثالثًا: البَصْمة الرَّقميَّة والتَّصيُّد الاحتياليّ.

02

أولًا: الثَّغَرات التي يَستغلّها مُنَفِّذُو هَجْمات التَّصيُّد الاحتياليّ

يمكن للمُهاجِمين الوصول إلى الأجهزة الخاصَّة بالمُسْتَخدِمين داخل المنزل وفي العمل وأيّ مكانٍ يوجد فيه ضحايا الهَجْمات السِّيبرانيَّة، وذلك من خلال خَرْق شبكة Wi-Fi الخاصَّة بالمُسْتَخدِمين أو الاستيلاء عن بُعْد على جهاز الحاسوب أو سرقة كلمات المرور بواسطة هَجْمات التَّصيُّد الاحتياليّ؛ الأمر الذي يتطلَّب تأمين الأجهزة الشَّخصيَّة، ويخترق المُهاجِمون الشَّبَكات والأجهزة من خلال استغلال نقاط الضَّعْف في أنظمة الأمان المُدمَجة بها، بغرض الوصول غير المُصَرَّح به إلى المعلومات الشَّخصيَّة، ونتيجةً لذلك يفقد ضحايا هَجْمات التَّصيُّد الاحتياليّ خصوصيَّتهم ويصبحون مُهدَّدين بسَرِقة الهُويَّة مدى الحياة.

وهناك عِدَّة طُرُق يَستغلّها المُهاجِمون السِّيبرانيُّون لخَرْق أجهزة المُسْتَخدِمين المُسْتَهدَفين الخاصَّة بهم، **وفيما يلي تبيان لأهمّها:**

- إرسال رسائل نصِّيَّة أو رسائل بريد إلكترونيّ مُزَيَّفة تحتوي على رَوابِط تَتَضمَّن برمجيَّات ضارَّة: وعند النَّقْر عليها يتمّ إصابة الأجهزة؛ مما يسمح للمُتَسلِّلين بالزَّحْف إلى جهاز الحاسوب الخاصّ بالمُسْتَخدِم للحصول على البيانات المُهمَّة أو بوَضْع برمجيَّات للتَّجسُّس على الجهاز.
- الاحتيال عَبْر الادِّعاء بتقديم الدَّعْم الفنِّيّ: حيث يتَّصلون بالمُسْتَخدِم المُسْتَهدَف عَبْر رسائل البريد الإلكترونيّ أو الدَّرْدشات مُدَّعين أنَّ الجهاز تعرَّض للخَرْق، وغالبًا ما يتمّ الاستعانة بأسماء مُؤَسَّسات معروفة في هذا المجال لإقناع المُسْتَخدِم.
- عدم تحديث المُسْتَخدِمين للبرامج والتَّطبيقات يجعل منها مَنْفذًا أمام المُهاجِمين للتَّسلُّل إلى الأجهزة الشَّخصيَّة، لذا يجب التَّيقُّظ لأهمِّيَّة تحديث البرامج أوَّلًا بأوَّل؛ للاستفادة من الإصلاحات التي تُجريها الشَّركات التِّقنيَّة بها لتأمينها.
- استخدام كلمات مرورٍ ضعيفةٍ سهلة التَّخمين.
- النَّقر على الرَّوابِط المجهولة أو غير الموثوق بها مِن قِبَل المُسْتَخدِمين يساعد المُهاجِمين على التَّسلُّل إلى أجهزتهم والتَّحكُّم بها عن بُعْد، أو نقلهم لموقع ويب مُزَيَّف يُسهِم في سَرِقة البيانات الشَّخصيَّة مِثْل كلمات المرور والأسماء وباقي التَّفاصيل الشَّخصيَّة.

وبِشَكْلٍ عامّ توجد العديد من الدَّلائل التي تشير إلى احتمال تَعرُّض الأجهزة الإلكترونيَّة للخَرْق، **فيما يلي تبيان لأهمّها:**

- تلقِّي إشعارات عَبْر البريد الإلكترونيّ حول محاولات تسجيل الدُّخول على حساباتك رَغْم عدم قيامك بذلك.
- بُطْء الجهاز وارتفاع درجة حرارته، وتأخُّر تنفيذ الأوامر التي يتلقَّاها من المُسْتَخدِم.
- ظهور نوافذ مُنْبَثِقة تحتوي على رسائل مُزْعِجة تَدَّعي إصابة جهازك الإلكترونيّ بالفيروسات.
- فَتْح نوافذ المُتَصَفِّح وعلامات التَّبويب والتَّطبيقات الموجودة على جهاز المُسْتَخدِم الخاصّ مِن تلقاء نفسها.
- تلقِّي اتِّصالٍ تحذيريّ من مكان العمل حول خَرْق البيانات.
- مُحاوَلات تسجيل دخولٍ غير ناجحةٍ إلى حساباتك.
- تلقِّي الأصدقاء وزُمَلاء العمل رسائل غير مألوفةٍ من المُسْتَخدِم المُسْتَهدَف.
- تلقِّي رسائل بريد عشوائيَّة في صندوق الوارد الخاصّ بالضَّحيَّة.
- إعادة توجيه المُسْتَخدِم المُسْتَهدَف باستمرارٍ إلى مَواقِع الويب غير المرغوب فيها في أثناء محاولته تصفُّح الإنترنت[1].

1. Warning signs you've been hacked and what to do next. On site: https://cutt.us/rd84U

ثانيًا: الأخطاء التي يرتكبها مُسْتَخْدِمُو الإنترنت

يمكن إيقاف الهجمات السّيبرانيَّة بواسطة سياسة أَمَان المحتوى، مثل هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS)، ما يُساعِد أصحاب مواقع الويب على تحديد الموارد الآمنة وغير الآمنة، وتُسْهِم تلك السِّياسات أيضًا في تمكين أصحاب مواقع الويب من وَضْع قواعدهم الخاصَّة التي تناسب احتياجات موقعهم، فضلًا عن كونها تَمْنَع وصول غير المُصرَّح لهم إلى المعلومات المهمَّة، وهذا بالإضافة إلى توفير أدوات إعداد التَّقارير والتَّحليلات التي تبحث عن الثَّغرات الأمنيَّة بعد تثبيت سياسة أَمَان المُحْتَوَى CSP.

هناك عِدَّة أخطاء يقع فيها مُسْتَخدِم الإنترنت خلال أداء مهامّه أو التَّصفُّح على الشَّبَكة العَالَميَّة، تَتَمثَّل في النِّقاط التَّالية:

1. التَّصفُّح على شبكة Wi-Fi عامَّة دون اتِّخاذ الاحتياطيَّات الأمنيَّة المطلوبة، ممَّا يجعلهم أكثر عُرْضة للخَرْق والوقوع ضحيَّة هَجْمات التَّصيُّد الاحتياليّ؛ حيث يصبح المُسْتَخدِم مُرَاقَبًا مِن قِبَل المُهاجِم لرصد تحرُّكاته على الإنترنت والحُصُول على كلمات المرور والبيانات الحسَّاسة، لذا يُفضَّل تجنُّب إجراء المعاملات الخاصَّة عَبْر الإنترنت عند استخدام شبكة Wi-Fi عامَّة.
2. عدم تحديث المُتَصَفِّح والتَّطبيقات الموجودة على الأجهزة، يجعل منها فرصة أمام المُهاجِمين للتَّسلُّل عَبْر الثَّغَرات الأمنيَّة الموجودة بالنُّسَخ القديمة، والتي تقوم الشَّركات التِّقنيَّة بتحديثها باستمرارٍ.
3. مشاركة المعلومات الشَّخصيَّة على وسائل التَّواصُل الاجتماعيّ، تعطي المُهاجِمين الفرصة لاستغلال تلك المعلومات لتنفيذ هَجْمات التَّصيُّد الاحتياليّ ضد المُسْتَخدِم.
4. تشابُه كلمات المرور لعددٍ من الحسابات عَبْر الإنترنت، ينتج عنه زيادة فُرَص تعرُّض المُسْتَخدِمين للاحتيال والسَّرِقة لأنَّ الوصول إلى أيّ منها يعني الوصول إلى باقي الحسابات.
5. استخدام كلمات مرور سهلة التَّخمين، ممَّا يُسهِّل عمليَّة خرقها، وهناك نوعان من كلمات المرور البسيطة التي يتمكَّن المُهاجِم من خرقها بسهولة، أوَّلهما: الكلمات أو الأرقام أو الرُّموز المتتالية مثل (123456، أ ب ج)، وثانيهما: المصطلحات الشَّائعة التي يسهل تخمينها سريعًا.

6. عـدم تثبيـت تحديثـات البرنامـج تلقائيًـا، ممّـا يزيـد مـن فُـرَص تسـلُّل الفيروسـات إلـى النّظـام، فمثـلًا تُوفِّـر مايكروسـوفت تحديثًـا مسـتمرًّا لنظامها الحاسـوبي ويندوز Windows، وهنا يُفضَّـل ضَبْـط جهاز الحاسـوب الخـاصّ بالمُسْـتَخدِم علـى "التّحديـث التّلقائـيّ" لضمـان الحُصُـول علـى كُلّ تحديـثٍ لنظـام Windows تلقائيًـا[1].
7. فَتْـح الرّوابِـط مـن رسـائل البريـد الإلكترونـيّ دون التّحقُّـق مـن موثوقيّتها يُمَكِّـن الفيروسـات والاختراقـات مـن التّسـلُّل إلـى الأجهـزة.
8. الانسـياق وراء الرّسـائل البريديّـة التـي تحتـوي علـى اسـتطلاعاتٍ أو فُـرَص هدايـا أو مُسـابَقات، دون التّحقُّـق مـن صحّتها عَبْـر البحـث علـى مُحَـرِّكات مثـل جوجـل Google عـن اسـم الشّـركة، بالإضافـة إلـى كلمـة "احتيـال" أو "مُراجعـة" Review للتّأكُّـد مـن عـدم ورود شَـكْوَى منهـا سـابقًا.
9. تجاهـل ميـزات الأمـان الأساسـيّة ومـن بينهـا المُصادَقـة الثُّنائيّـة، فهـذه الخُطُـوات تضمـن حمايـة كلمـات المـرور فـي حـال محاولـة أحـد المُتَسـلِّلين خـرق حسـاباتك؛ إذ يتلقّـى المُسْـتَخدِم حينهـا إشـعارًا يفيـد بذلـك علـى هاتفـه أو بريـد آخـر لـه.
10. التّسـوُّق عَبْـر الإنترنـت مـن مَواقِـع غيـر مَوْثوقـة، يزيـد مـن فُـرَص تعـرُّض المُسْـتَخدِم للخـرق، خاصّـةً إذا اسـتخدم بطاقاتـه البنكيّـة الشّـخصيّة. لـذا يُفضَّـل اسـتخدام بطاقـة بِسِـعَةٍ محـدودة مـن المـال، مـع وَضْـع كلمـة سـرّ قويّـة يَصْعـب تخمينهـا للتّغلُّـب علـى محـاولات الاحتيـال التـي تحـدث.
11. ينتشـر علـى وسـائل التّواصُـل الاجتماعـيّ خاصّـةً Facebook الكثيـر مـن الاختبـارات المُغْرِيـة مثـل "إذا لـم تكـن محاميًـا تخيَّـل مـاذا سـتكون؟" وبِمُجـرَّد زيـارة المُسْـتَخدِم لهـذه الصّفحـات التـي تُنَفِّـذ الاختبـارات يصبـح فريسـةً للاحتيـال والسّـرِقة.
12. عـدم الاسـتفادة مـن إعـدادات الخصوصيّـة الخاصّـة بـك علـى وسـائل التّواصُـل الاجتماعـيّ، فتصبـح جميـع الصُّـوَر والمعلومـات والمُشـارَكات متاحـة للجميـع مـن المُقَرَّبيـن للمُسْـتَخدِم وأيضًـا الغُرَبـاء[2].

1. Which 7 Online Mistakes Will You Make Today? On site: https://cutt.us/z25Nk
2. 10 mistakes people make online. On site: https://cutt.us/4XQ7A

ثانيًا: البَصْمة الرَّقميَّة والتَّصيُّد الاحتياليّ

يُقصَد بالبَصْمة الرَّقميَّة (الإلكترونيَّة) أنَّها مسار البيانات التي يتركها المُسْتَخدِم عند استخدام شبكة الإنترنت، مثل المَواقِع التي يزورها ورسائل البريد الإلكترونيّ وعمليَّات التَّسوُّق والمُحادَثات (الدَّرْدشات)، وجميع التَّحرُّكات التي يقوم بها المُسْتَخدِم عَبْر حساباته المُخْتَلِفة أيًّا كانت تلك التَّحرُّكات جيِّدة أَمْ لا؛ وقد تسهم مَواقِع الإنترنت في تشكيل بَصْمة المُسْتَخدِم الرَّقميَّة من خلال تثبيت «ملفَّات تعريف الارتباط» على أجهزته، كما يمكن للتَّطبيقات جَمْع البيانات الخاصَّة بالمُسْتَخدِمين دون عِلْمهم وذلك في حال سمحوا لها بالوصول إلى المِلفَّات المُخَزَّنة سواءٌ كانت نصِّيَّة أو فيديوهات أو صورًا أو غيرها.

وهناك نوعان من البَصْمة الرَّقميَّة هما البَصْمة النَّشِطة، والبَصْمة الخَامِلة، وتُعرَف البَصْمة الرَّقميَّة النَّشِطة بأنَّها:

نَشْر المُسْتَخدِم عَمْدًا المعلومات والبيانات الخاصَّة به علنًا مثلما يحدث على وسائل التَّواصُل الاجتماعيّ، أو دخوله إلى مَواقِع الإنترنت من خلال البيانات التَّعريفيَّة مثل (اسم المُسْتَخدِم وكلمة السِّرّ)، أو إكمال نموذج بيانات عَبْر الإنترنت مثلما يحدث عند الاشتراك في الخِدْمات الإخباريَّة أو الوظائف، وغيرها[1].

أمَّا البَصْمات الرَّقميَّة السَّلبيَّة فيُقصَد بها ما يتمّ جَمْعه من معلوماتٍ عن المُسْتَخدِمين دون عِلْمهم، مثل تجميع مَواقِع الإنترنت لمعلوماتٍ عن عدد الزِّيارات والصَّفحات التي تمّ زيارتها، وعدد المُشاهَدات على أحد الفيديوهات وعناوين IP، وكذلك استفادة الجهات الإعلانيَّة من تسجيلات الإعجاب والمُشارَكات والتَّعليقات التي يقوم بها المُسْتَخدِم بِشَكْلٍ عَفَويّ من أجل توجيه محتويات تتناسب مع اهتماماته فيما بعد[2].

1. What is a digital footprint? And how to protect it from hackers. On site: https://cutt.us/bObsJ
2. digital footprint. On site: https://cutt.us/P2gI8

للبَصْمة الرَّقميَّة أهمِّيَّة واضحة في عِدَّة مجالات، فيما يلي تبيان لأبرزها:

- تكون دائمةً ويصعب السَّيطرة على كيفيَّة استخدام الآخرين لها.
- تُحدِّد السُّمْعة الرَّقميَّة للمُسْتَخدِم كما هو الحال خارج الإنترنت.
- يمكن لأصحاب العمل والجامعات التَّحقُّق من البَصْمات الرَّقميَّة للمُوظَّفين والطُّلَّاب المُحْتَمَلين، وخاصَّةً عَبْر وسائل التَّواصُل الاجتماعيّ قبل اتِّخاذ قرار التَّوظيف أو قبول أوراق الالتحاق بالجامعة.
- يمكن إساءة تفسير الكلمات والصُّوَر ومقاطع الفيديو التي يتمّ مشاركتها.
- الإضرار بالعلاقات الاجتماعيَّة بين الأفراد نتيجة مشاركة محتويات المجموعات الخاصَّة عبر الإنترنت بِشَكْلٍ عامّ.
- يمكن للمُتَسَلِّلين الإلكترونيِّين استغلال البَصْمة الرَّقميَّة في عمليات التَّصيُّد الاحتياليّ أو في إنشاء هُوِيَّات مُزَيَّفة وَفْق البيانات المُجَمَّعة من البَصْمة[1].

ويمكن للمُسْتَخدِم الإسهام في تشكيل بَصْمته الرَّقميَّة من خلال المُمارَسات الرَّقميَّة التَّالية:

- التَّسوُّق عَبْر الإنترنت.
- التَّسجيل في النَّشرات البريديَّة بالمَواقِع الإلكترونيَّة.
- المُعامَلات الماليَّة عَبْر الإنترنت.
- وسائل التَّواصُل الاجتماعيّ.
- الانضمام إلى المَواقِع الإلكترونيَّة.
- الاشتراك في النَّشرات الإخباريَّة.
- الاشتراك في التَّطبيقات المُخْتَلِفة.

1. Importance of Digital Footprint: Complete Guide [2023]. On site: https://cutt.us/DCq7d

وبِشَكْلٍ عامّ ينبغي للمُسْتَخدِم حماية بَصْمته الرَّقميَّة، وهناك عِدَّة طُرُق للقيام بذلك، فيما يلي تبيان لأهمّها:

- التَّحقُّق من البَصْمة الرَّقميَّة الخاصَّة بنا عَبْر مُحَرِّكات البحث، ويتمّ ذلك عَبْر إدخال الاسم والبحث عنه على المُحَرِّك لرُؤْية ما يظهر في نتائج البحث.
- إزالة المعلومات الشَّخصيَّة من المَواقِع غير المُهمَّة، مِثْل مَواقِع اللِّياقة البدنيَّة لتقليل تداول تلك المعلومات عبر الإنترنت.
- السَّيطرة على كمِّيَّة المعلومات التي يتمّ مشاركتها عَبْر وسائل التَّواصُل الاجتماعي، وباقي المَواقِع.
- ضَبْط إعدادات الخصوصيَّة، بحيث تُقيِّد مَنْ يمكنه رُؤْية بياناتك أو تسجيل الإعجاب والتَّعليق على منشوراتك ورُؤْية صُوَرك.
- التَّحقُّق من المَواقِع التي يتمّ زيارتها، أو التي تصل رَوابِطها إلى البريد الإلكترونيّ؛ لأنَّها قد تكون للتَّصيُّد الاحتياليّ ولسَرِقة البيانات الحسَّاسة، فينبغي التَّأكُّد من بَدْء عنوان المَوْقِع بـ https فحرف s هنا يدلّ على أمان المَوْقِع.
- عدم استخدام شبكات Wi-Fi عامَّة، عند إجراء المعاملات الماليَّة أو الشَّخصيَّة.
- حَذْف الحسابات القديمة، من إحدى الوسائل التي تُقلِّل من المعلومات المُتَداوَلة عن المُسْتَخدِمين عبر الإنترنت.
- إنشاء كلمات مرور قويَّة ومُخْتَلِفة للحسابات.
- عدم تسجيل الدُّخول إلى المَواقِع أو التَّطبيقات بواسطة بيانات Facebook.
- تحديث البرامج والتَّطبيقات، للاستفادة من الإصلاحات الأمنيَّة التي تجريها الشَّركات التِّقنيَّة عليها أوَّلًا بأول.
- تعيين كلمة مرور للهاتف الذَّكيّ، حتَّى لا يتمّ استغلال البيانات الموجودة عليه في حال فَقْده أو خَرْقه أو سَرِقته.
- عند التَّعرُّض للخَرْق يجب تغيير كلمات المرور لجميع الحسابات فورًا.

الفَصْل الثَّالث

كيفيَّة التَّصرُّف في حال التَّعرُّض لِتَصيُّد احتياليّ

- أوَّلًا: إرشادات الحماية من التَّصيُّد الاحتياليّ.
- ثانيًا: حماية البيانات من القَرْصنة.
- ثالثًا: ماذا أفعل عند تعرُّضي للتَّصيُّد الاحتياليّ؟

0 3

أوَّلًا: إرشادات الحماية من التَّصيُّد الاحتياليّ

يستخدم المُهاجِمون السّيبرانيُّون البريد الإلكترونيّ أو الرَّسائل النَّصّيَّة لمحاولة سَرِقة كلمات المرور أو أرقام الحسابات البنكيَّة الخاصَّة بالمُسْتَخدِمين، وهم يشنون الآلاف من هَجْمات التَّصيُّد الاحتياليّ التي ينجح معظمها في تحقيق هدفه. ولتجنُّب مثل هذه الهَجْمات الاحتياليَّة، ينبغي تجنُّب النَّقْر على الرَّوابِط أو المُرْفَقات المُرسَلة في رسائل البريد الإلكترونيّ مجهولة المصدر أو غير المُتَوقَّعة، وفي حال تلقِّي إشعاراتٍ مُتكرِّرةٍ عن محاولة تسجيل الدُّخول لحسابات المُسْتَخدِم، يجب عليه تغيير كلمة المرور فورًا في جميع الحسابات شرط أن تكون الكلمة قويَّة وطويلة. وبِشَكْلٍ عامّ هناك دلائل تُميِّز رسائل البريد الإلكترونيّ الاحتياليَّة، **فيما يلي تبيان لأهمّها:**

- تحتوي الرَّسائل على لُطْفٍ مُبالَغ فيه.
- تدعو الرَّسائل المُسْتَخدِم للنَّقْر على رابطٍ لتحديث بيانات الحسابات الخاصَّة به.
- كثرة الأخطاء الإملائيَّة والنَّحويَّة برسائل البريد.

كيف تحمي نفسك من هَجْمات التَّصيُّد؟

لا تفيد دائمًا عمليَّة تصفية البريد العشوائيّ في التَّخلُّص من جميع الرَّسائل الاحتياليَّة بسبب تحايُل المُهاجِمين للوصول إلى المُسْتَخدِم، ومن طُرُق الحماية:

- استخدام برامج الأمان وبرامج مُكافَحة البرمجيَّات الضَّارَة والفيروسات لحماية الحواسيب والأجهزة الذكيَّة، مع تعيين التَّحديث التِّلقائيّ للبرامج والتَّطبيقات لتَتَمكَّن من مُواجَهة التَّهديدات السّيبرانيَّة.
- وَضْع كلمة سرّ للهاتف الذَّكيّ، مع ضَبْط التَّحديث التِّلقائيّ لبرامجه.
- استخدام المُصادَقة الثُّنائيَّة لتوفير أمانٍ إضافي للحسابات، سواءً بواسطة رَمْز مرور أو الإجابة عن سؤالٍ ما أو ببصمة الإصبع أو الوجه. عمل نُسْخةٍ إضافيَّةٍ من البيانات المُخَزَّنة، ووَضْعها في مكانٍ آخر بخلاف جهاز الحاسوب لإمكانيَّة استرجاعها إذا تعرَّض الجهاز للخَرْق[1].

1. How to Recognize and Avoid Phishing Scams. On site: https://cutt.us/0VwNx

ثانيًا: حماية البيانات من القَرْصنة

مع تزايد الاختراقات الأمنيَّة للأجهزة الإلكترونيَّة في العالم وسَرِقة البيانات والحسابات، زادت الحاجة إلى توفير الأمن لها، ويمكن تلخيص طُرُق حماية البيانات من السَّرِقة في الآتي:

- استخدام برامج مُكافَحة الفيروسات، فهي تُمثِّل خطّ الدِّفاع الأوَّل ضِدّ الهَجْمات الاحتياليَّة، لكَوْنها تحمي الأجهزة من التَّسلُّل وتتعامل مع البرمجيَّات الضَّارَّة التي يستغلّها المُهاجِمون للوصول إلى البيانات والمِلفَّات.
- تفعيل المُصادَقَة الثُّنائيَّة، فهي الطَّريقة المُثْلى لحماية الحسابات من الدُّخول غير المُصَرَّح به وسَرِقة البيانات سواءً تمّ ذلك برُمُوز أو بَصْمة الإصبع أو الوجه، أو بالإجابة عن الأسئلة؛ فكُلّها أمور تُصعِّب عمليَّة الخَرْق.
- تحديث أنظِمَة التَّشغيل والبرامج والتَّطبيقات أمرٌ ضروريّ نظرًا لإدخال تعديلاتٍ دائمةٍ عليها مِنْ قِبَل الشَّركات التِّكنولوجيَّة المُنْتِجة لِسَدّ أيّ ثغراتٍ أمنيَّةٍ تظهر بها، فتلك الثَّغرات تُمثِّل بوَّابة عبور المُتَسلِّلين إلى الأجهزة ومِنْ ثَمَّ إلى الحسابات والمِلفَّات المُخَزَّنة على الأجهزة.
- بجانب الطُّرُق السَّابقة، يجب وَضْع نُسْخة احتياطيَّة من البيانات في مكانٍ آخر بعيد عن الجهاز الشَّخصيّ لحمايتها في حال تمّ خَرْق الجهاز أو ضياعها أو إتلافها، ويمكن هنا الاستفادة من الحَوْسبة السَّحابيَّة، لكنْ يُفَضَّل أيضًا الاحتفاظ بنسخةٍ أخرى في مكانٍ آخر.
- التَّثقيف بمبادئ الأمن السِّيبرانيّ، تُسهِم تلك الخُطْوة في حماية الأفراد من الوقوع في فخّ التَّصيُّد الاحتياليّ وغيرها من هَجْماتٍ سيبرانيَّةٍ هدفها الأساسيّ إلْحاق الضَّرَر بِمُسْتَخدِمي الإنترنت.
- تجنُّب استخدام شبكة Wi-Fi عامَّة (مجانيَّة) قَدْر الإمكان على الجهاز الشَّخصيّ.
- التَّحقُّق من الرَّوابِط المُرْسَلة بالبريد قبل النَّقْر عليها.
- إيقاف تشغيل Bluetooth على الجهاز الشَّخصيّ في حالة عدم الحاجة إليه.
- تقليل البَصْمة الرَّقميَّة وتفعيل إعدادات الخصوصيَّة لوسائل التَّواصُل الاجتماعيّ[1].

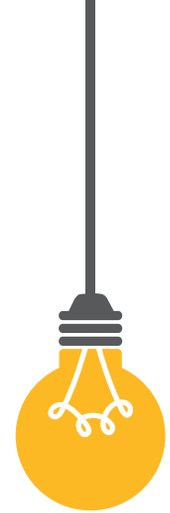
1. 18 Ways to protect your data from hackers. On site: https://cutt.us/3M0uz

ثالثًا: ماذا أفعل عند تعرُّضي للتَّصيُّد الاحتياليّ؟

في حالة التَّعرُّض للتَّصيُّد الاحتياليّ يمكن القيام بإحدى الإجراءات التَّالية، ويمكن اللُّجوء لعددٍ من الجهات التي من الممكن أن تُقدِّم مساعدة في هذا المجال، **وفيما يلي تبيان لأهمّ هذه الإجراءات:**

- في حالة شَكّ المُسْتَخدِم بتعرُّضه لهجوم تصيُّد احتياليّ مثل رسالة بريد مُزَيَّفة، فإذا كان لديه تعامل مع الأفراد أو الجهات المُدْرَجة في الرَّسائل، فعليه التَّواصُل معها شخصيًّا عَبْر الأرقام المُعْتَمَدَة أو الحسابات الرَّسميَّة.
- أما في حالة فَتْح أيّ مُرْفَقٍ أو رابطٍ برسالة البريد الإلكترونيَّة الاحتياليَّة، فهنا يجب على المُسْتَخدِم الاتِّصال بالبنك ووَقْف بطاقته الائتمانيَّة إذا شَكّ أنَّها مُعرَّضة للسَّرِقة.
- وفي حالة خَرْق جهاز الحاسوب الخاصّ بالمُسْتَخدِم، فهنا عليه التَّحرُّك سريعًا وفَصْل الاتِّصال بشبكة Wi-Fi الخاصَّة به، مع تفعيل برامج مُكافَحة الفيروسات للبحث عن البرمجيَّات الضَّارَّة وحَذْف التَّطبيقات المشكوك فيها.
- لا بُدّ من تحديث أنظمة التَّشغيل الخاصَّة به، وإعادة تعيين كلمات المرور جميعها وتفعيل المُصادَقة الثُّنائيَّة ومَسْح الجهاز والبَدْء في التَّثبيت من جديدٍ.
- تحذير الأصدقاء وأفراد العائلة وزملاء العمل والمدرسة بإمكانيَّة تلقِّيهم رسائل احتياليَّة من خلال تعرُّضك للخَرْق، وذلك لتجنيبهم التَّعرُّض لهَجْمات التَّصيُّد الاحتياليّ.
- إجراء فحص مُتقدِّم دون الاتِّصال بالإنترنت بواسطة برنامج الأمان المُدْمَج في نظام ويندوز Windows، من خلال فتح الإعدادات الخاصَّة بالمُسْتَخدِم على جهاز الحاسوب والانتقال إلى قائمة إعدادات الأمان ثمَّ تحديد «الحماية من الفيروسات والتَّهديدات» للبَدْء في إجراء فَحْصٍ شاملٍ لمكافحة الفيروسات، وغيرها من برمجيَّاتٍ خبيثةٍ على الجهاز دون الحاجة للاتِّصال بالإنترنت.
- الاستفادة من خِدْمات الدَّعم الفنِّيّ المُقدَّمة من شركات التِّكنولوجيا مثل مايكروسوفت Microsoft عَبْر الاتِّصال بالرَّقم المُعْتَمَد أو وسائل الاتِّصال المُعْلَن عنها، والأمر نفسه لباقي الشَّركات التِّقنيَّة مثل ماك Mac وأبل Apple.
- يُفضَّل التَّواصُل مع الجهات المَعْنيَّة بمُكافَحة الجرائم السِّيبرانيَّة داخل الدَّولة عند التَّعرُّض لأحد أنواع التَّصيُّد الاحتياليّ لامتلاك هذه الجهات الأجهزة والكفاءات التي تُمكِّنها من التَّدخُّل ومُعالَجة المشكلة قبل تفاقمها، واستعادة البيانات وتوقيف المُتَسلِّلين السِّيبرانيِّين[1].

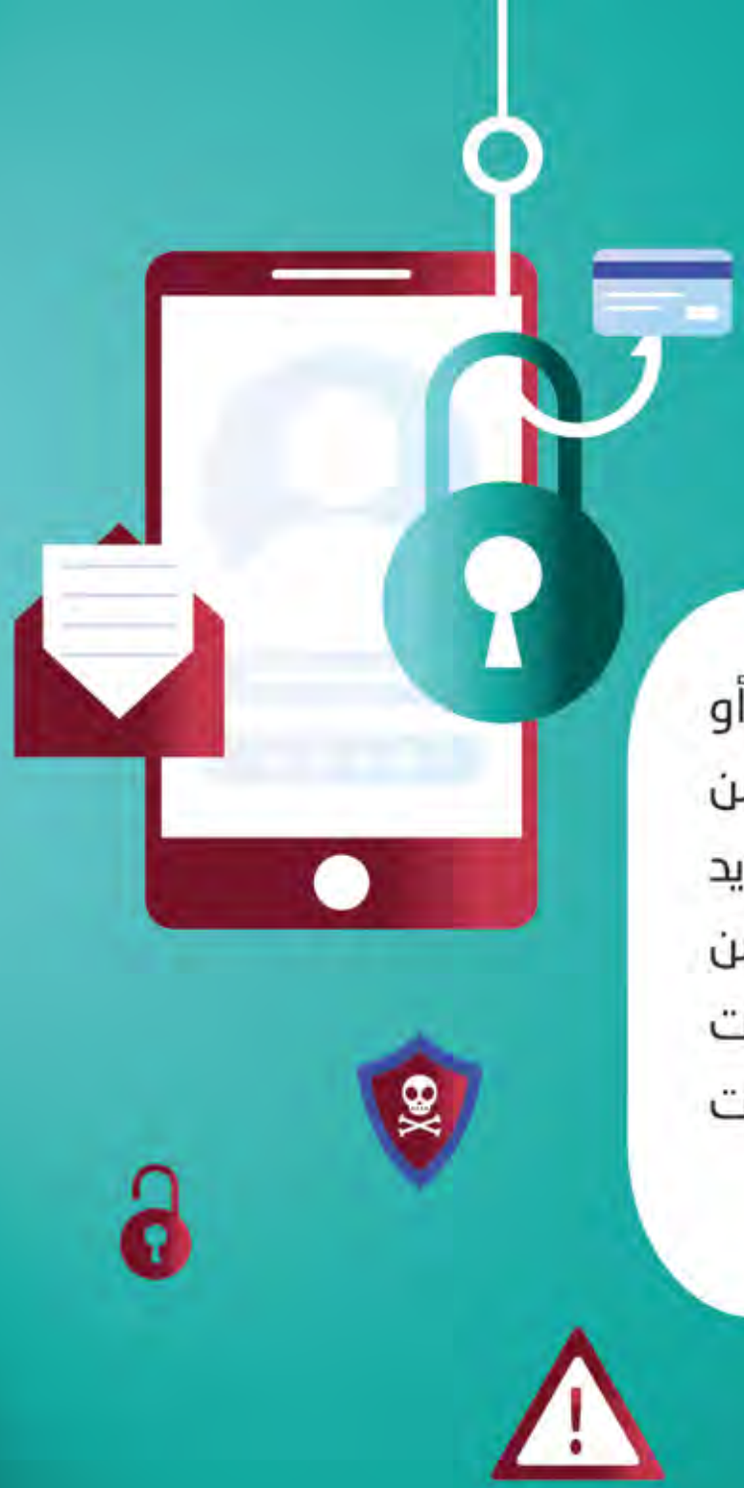
1. What to Do If You Give Your Personal Information to a Phisher. On site: https://cutt.us/axv7k



تمارين وتَدْريبَات

أولًا: التَّمَارين الصَّفِّيَّة

التَّدريبات هنا مَرْفَقَة بالحَلّ، بينما في كُتَيِّب الطَّالِب مَكْتُوبة بدون حَلّ، ومَرْفَق معها تَوجيه للطَّالب لكيفيَّة الحلّ، وذلك حيث تقتضي الضَّرورة.



انتَبِه!
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 المُرفَقات 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 الهاتفيّة؛ بغرض الحصول على أموال الضَّحايا أو المعلومات الشَّخصيّة 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 بالتَّصَيُّد الاحتياليّ:

التَّصَيُّد الاحتياليّ هو محاولة لسرقة الأموال أو الهويّات من خلال كشف المعلومات الشَّخصيَّة.	صحيح
يهتمّ منفذو التَّصَيُّد الاحتياليّ بالمعلومات السِّرِّيَّة، مثل منشورات منصَّات التَّواصل الاجتماعيّ.	خطأ
التَّصَيُّد الاحتياليّ يعتمد على كشف المعلومات السِّرِّيَّة، التي تشمل أرقام البطاقات الائتمانيَّة وكلمات السِّرّ والمعلومات البنكيَّة.	صحيح
أحيانًا تقوم مواقع إلكترونيَّة بعمليّات التَّصَيُّد الاحتياليّ.	صحيح
لا يَسْرق منفذو التَّصيُّد الاحتياليّ هَويَّة أحَد الأصدقاء أو أفراد الأُسْرَة.	خطأ
تُستخدَم الرَّسائل المزيَّفة في عمليّات التَّصَيُّد الاحتياليّ.	صحيح
الرَّوابط المشبوهة من أبرز طرق التَّصَيُّد الاحتياليّ.	صحيح
لا يمكن لمنفذي التَّصَيُّد الاحتياليّ الاستفادة بالمعلومات البنكيَّة أو أرقام البطاقات الائتمانيَّة.	خطأ
لا يهتمّ مُجْرمو التَّصَيُّد الاحتياليّ بالهويَّة.	خطأ
لا يمكنك حماية نفسك من التَّصَيُّد الاحتياليّ مهما حاولت.	خطأ

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!

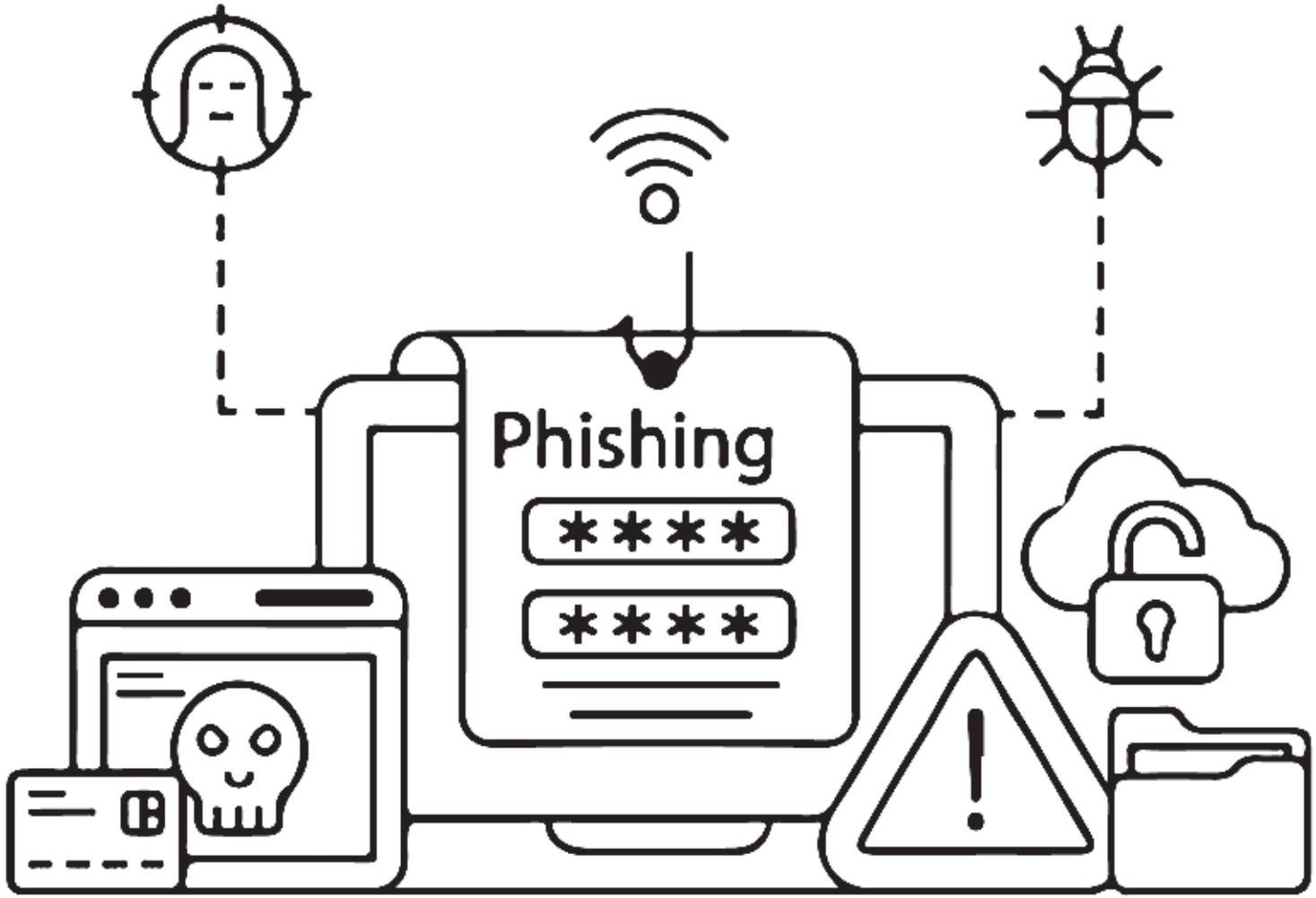
التَّصَيُّد عبر البريد الإلكترونيّ

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.

التّمرين الثّاني

ضَع الكلمة المناسبة لكلّ تعريف

هو الشّكل الأكثر شيوعًا للتّصَيُّد الاحتياليّ، ويستخدم برامج البريد الإلكترونيّ للنّصب والسّرقة.	التّصَيُّد عبر البريد الإلكترونيّ.
نوع من البرمجيّات الضّارّة التي يتمّ إخفاؤها في مَرْفق من المَرْفقات التي تَصِل إليك عبر البريد الإلكترونيّ وبمجرّد فتحها تتسبّب في تعطيل أنظمة التّشغيل.	الفيروسات.
نوع من هجمات التّصَيُّد الاحتياليّ تَستهدِف الشّبكات الكبيرة، أو مجموعة أشخاص بعينهم من خلال استغلال أبحاث أُجْرِيت عنهم وعن عملهم وحياتهم الاجتماعيّة.	التّصيُّد الاحتياليّ المُوَجّه.
تُستخدَم فيه الرّسائل القصيرة وتأتي متخفّية في هيئة علامات تجاريّة أو مواقع كبيرة موثوق بها؛ لخداع المُستخدِم لفتح الرّابط أو النّصّ المُرسَل.	التّصيُّد الاحتياليّ عَبْر الرّسائل القصيرة.
يُستخدَم فيه الصّوت لدَفْع الضّحيّة للإدلاء بمعلومات حسّاسة وشخصيّة عبر الهاتف، من خلال سرقة هويات شخصيات مُقرّبة من الضّحايا.	التّصيُّد الصّوْتيّ.


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

أكمِل الجمل التَّالية:

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

2. يَحْرِص المُتصيِّدون على **استغلال** حاجة الضَّحايا من أجل **الإيقاع بهم** ، وغالبًا ما يَقَع الباحثون عن عملٍ في هذا الفَخّ، فيُسرِعُون بتسجيل **الدُّخول** دون التَّحقُّق من الموقع، وبالطَّبع تُستَغلّ تلك البيانات ضدَّهم.

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

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

التّمرين الرّابع

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

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

التَّمرين الخامس

ضَعْ علامَة (✓) أو علامة (✗) أمام العبارات التَّالية:

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

6. تجنُّب استخدام برامج الحماية والجدران النّاريّة.

7. إرسال الأموال إلى الجمعيّات الخيريّة التي تتواصل معك دون التّأكُّد منها.

8. مُشارَكة بيانات بطاقاتك البنكيّة على مواقع التّسوُّق الإلكترونيّ كلّها.

9. تَجنُّب الإفصاح عن أيّ بيانات شخصيّة أو معلومات حسّاسة تخصُّك.

10. الرُّجوع إلى البنك قبل الإفصاح عن أيّ بيانات خاصّة من المكالمات التي تدّعي أنّها 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 الاحْتِيَالِيّ؛ حيث يتمّ تصميم موقع ويب مُزيَّف، ثم إعادة توجيه المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ إليه لسرقة المعلومات السِّرِّيَّة.

التَّمرين السَّادس

عمليّات الشِّراء الإلكترونيّة.	✓
التَّسجيل في المواقع الإلكترونيّة.	✓
تحميل التَّطبيقات من مَتاجِر التَّطبيقات.	✓
التَّحدُّث عبر الهاتف.	✗
التَّسجيل في النَّشرات العامَّة.	✓
الذَّهاب في نزهة.	✗
بيع وشراء الأسهم.	✗
الاشتراك في المجلّات الإلكترونيَّة.	✓
فتح حساب بنكيّ.	✗
منشورات منصّات التَّواصل الاجتماعيّ.	✓
مشاهدة برامج على التِّلفاز.	✗
مشاركة المعلومات والصُّور مع الأصدقاء.	✓
إعادة نَشْر المقالات والمعلومات التي تقرأها.	✓
الاشتراك في المُدوَّنات الصِّحِّيَّة.	✓
نَشْر المقاطع المُصَوَّرة عبر منصّات 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 ضارّ ما, يتسبَّب في إصابة أجهزة الحاسوب الخاصَّة بهم.


ثانيًا: التَّمارين اللَّاصَفِّيَّة

انْتَبِه!

التَّصيُّد الاحْتِيَالِيّ 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 الاحْتيَاليّ الموجَّه لكبار الشَّخصيّات

هو هجوم تَصيُّد احْتيَاليّ يَستهدف كبار المسؤولين التَّنفيذيّين 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 الاحْتيَاليّ 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

استخرج الكلمات التَّالية من 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	ى	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 حقيقيّة أم مجرّد تصيّدٍ احتياليّ؟ وكيف ستتصرّف حيالها؟

تُعدّ الإجابة صحيحة في حالة ذَكَر الطّالب معلوماتٍ حول ضرورة التّأكّد من الجهة التي أرسلت الرّسالة، وعدم فَتْح الرّسالة في حال وجود شَكّ بأنّها مُزَيّفة، إضافةً لذِكْره معلومات حول تجاهل الرّسائل المشكوك فيها وعدم فَتْحها.

التّمرين الثّالث

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

في حالة أجاب الطّالب عن معرفته بأحدٍ تعرّض لهجوم تصيُّد احتياليّ، تُعدّ إجابته صحيحة في حالة ذِكْر معلومات عن كيفيّة التّصرُّف الصّحيح، بما يشمل إيقاف التّواصُل مع المحتال، وإعلام البنك أو المُؤَسّسة التي يتمّ استغلال اسمها وإعلام الجهات الرّسميّة المسؤولة عن الجرائم الإلكترونيّة، أو أيّ معلومات تتقاطع بِشَكْلٍ مُباشِرٍ أو غير مُباشِرٍ مع هذه المعلومات.


01001110
01110100
0111011101
11110001011

التَّمرين الرَّابع

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

تحقَّق من المَرسِل، خاصَّةً في أثناء فتح رسائل البريد الإلكترونيّ التي تحتوي على مُرفَقات.	✓
قُمْ بفتح أيّ رسالة بريد إلكترونيّ من أيّ شخص حتى لو لم تكن تعرفه.	✗
قَدِّم بلاغًا لمزوِّدي الخدمة حيال البريد الإلكترونيّ المَشْبوه.	✓
قُمْ بالرَّدِ على أيّ مكالمات أو رسائل تَطْلُب بياناتك الشَّخصيَّة؛ حيث لا ضرر في ذلك.	✗
مرِّر المؤشِّر على الرَّابط للتَّأكُّد من أنَّه موقع حقيقيّ قبل الدُّخول عليه.	✓
شارِك في العروض التَّرويجيَّة واترك بريدك الإلكترونيّ في كلّ المواقع والمنصَّات.	✗
لا بأس في زيارة مواقع الإنترنت الغريبة أو ذات الامتدادات غير المعروفة.	✗
ابحث عن الأخطاء النَّحويَّة أو الإملائيَّة؛ لأنَّها مؤشِّر مهمّ للرَّسائل المزيَّفة.	✓
في حالة التَّعرُّض لهجوم أو خَرْق، لا تقلق، وإياك أن تُبْلِغ الجِهات المسؤولة.	✗
لا تَشْغَل بالك بتحديث الأنظمة أو التَّطبيقات الموجودة على حاسوبك أو هاتفك.	✗

التَّمرين الخامس

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

1. لا تُشارِك بيانتك الشَّخصيَّة مع أيّ جهةٍ كانت.
2. لا تدخل إلى المَواقِع أو الرَّوابِط المشبوهة.
3. احرِص على تحديث برامج تشغيل الجهاز.
4. احرِص على تثبيت برامج مَكافَحة الفيروسات.
5. تَواصَل مع إدارة مكافحة الجرائم الإلكترونيَّة بوزارة الدَّاخليَّة في حالة تعرَّضك لعمليَّة تصيُّد أو احتيال عبر الإنترنت.

التمرين السّادس

عَرِّف المصطلحات التّالية

الهندسة الاجتماعيّة ..... تقنيّة حديثة تعتمد على الغرائز البشريّة الطّبيعيّة مثل الثّقة أو الخَوْف، وغيرها من مشاعر يستغلّها المُهاجمون السّيبرانيّون للتّأثير في الضّحايا لدَفْعهم إلى اتّخاذ قرارٍ مُعيّن يقود إلى تحقيق هدف المُهاجم مثل سَرِقة المال أو المعلومات الحسّاسة.

كلمة المرور ..... مجموعة من الأَحْرُف والرّموز التي تستخدم لحماية البريد الإلكترونيّ والحسابات المَصْرفيّة وحسابات مَواقِع التّواصُل الاجتماعيّ، بحيث لا تسمح لأحدٍ غير صاحب هذه الحسابات باستخدامها أو الاطّلاع على محتواها.

التّصَيُّد الاحتياليّ ..... أحد أنواع الجَرائم الرّقميّة الأكثر انتشارًا، وفي هذا النّوع يتمّ استغلال شَبَكة الإنترنت لخداع الضّحايا المُسْتَهدَفين لسَرِقة بياناتهم الشّخصيّة مثل كلمات المرور وأرقام بطاقات الائتمان، وذلك من خلال طُرُق وأدوات عِدّة، منها إنشاء موقع إلكترونيّ مُزَيَّف لاستدراج الضّحيّة؛ وإرسال الرّابط عَبْر البريد الإلكترونيّ أو رسائل الماسنجر للضّغط عليها، ومِنْ ثَمّ السّماح للقراصنة دون علم المُسْتَخدِم بالدّخول غير المشروع إلى حسابات وأجهزة الضّحايا وتثبيت بَرامِج خبيثة تساعدهم في سَرِقة البيانات.

البَصْمة الرّقميّة ..... مسار البيانات التي يتركها المُسْتَخدِم عند استخدام شَبَكة الإنترنت، مثل المَواقِع التي يتمّ زيارتها ورسائل البريد الإلكترونيّ وعمليّات التّسوُّق والمُحادَثات (الدَّرْدشات)، وجميع التّحرُّكات التي يقوم بها المُسْتَخدِم عَبْر حساباته المُخْتَلِفة أيًّا كانت تلك التّحرُّكات جيّدة أَمْ لا؛ وقد تُسهِم مَواقِع الإنترنت في تشكيل بَصْمة المُسْتَخدِم الرّقميّة من خلال تثبيت "مِلفّات تعريف الارتباط" على أجهزته، كما يمكن للتّطبيقات جَمْع البيانات الخاصّة بالمُسْتَخدِمين دون عِلْمهم، وذلك في حالة سمحوا لها بالوصول إلى المِلفّات المُخَزّنة سواءً كانت نصّيّة أو فيديوهات أو صُوَرًا، أو غير ذلك.

الاحتيال عبر الإنترنت ..... تنكُّر المُهاجِمين الرّقميّين في شخصية كيان معروف كإحدى الشّركات المعروفة ذات السُّمْعة الجيّدة أو شخص حَسَن السُّمْعة وإرسال رسالة بريد إلكترونيّ أو أيّ شَكْلٍ آخر من أشكال الاتّصال، وعادةً ما يستخدم المُهاجِمون رسائل البريد الإلكترونيّ الاحتياليّة لتوزيع الرّوابط أو المُرْفَقات الضّارّة التي من خلالها يحصل المُهاجِم على بياناتٍ حسّاسةٍ تهمّ الضّحيّة مثل بيانات اعتماد تسجيل الدّخول، أو أرقام الحسابات البنكيّة، أو المعلومات الشّخصيّة الخاصّة بالعائلة أو العمل.

أهداف هجمات التَّصيُّد الاحْتِيَالِيّ

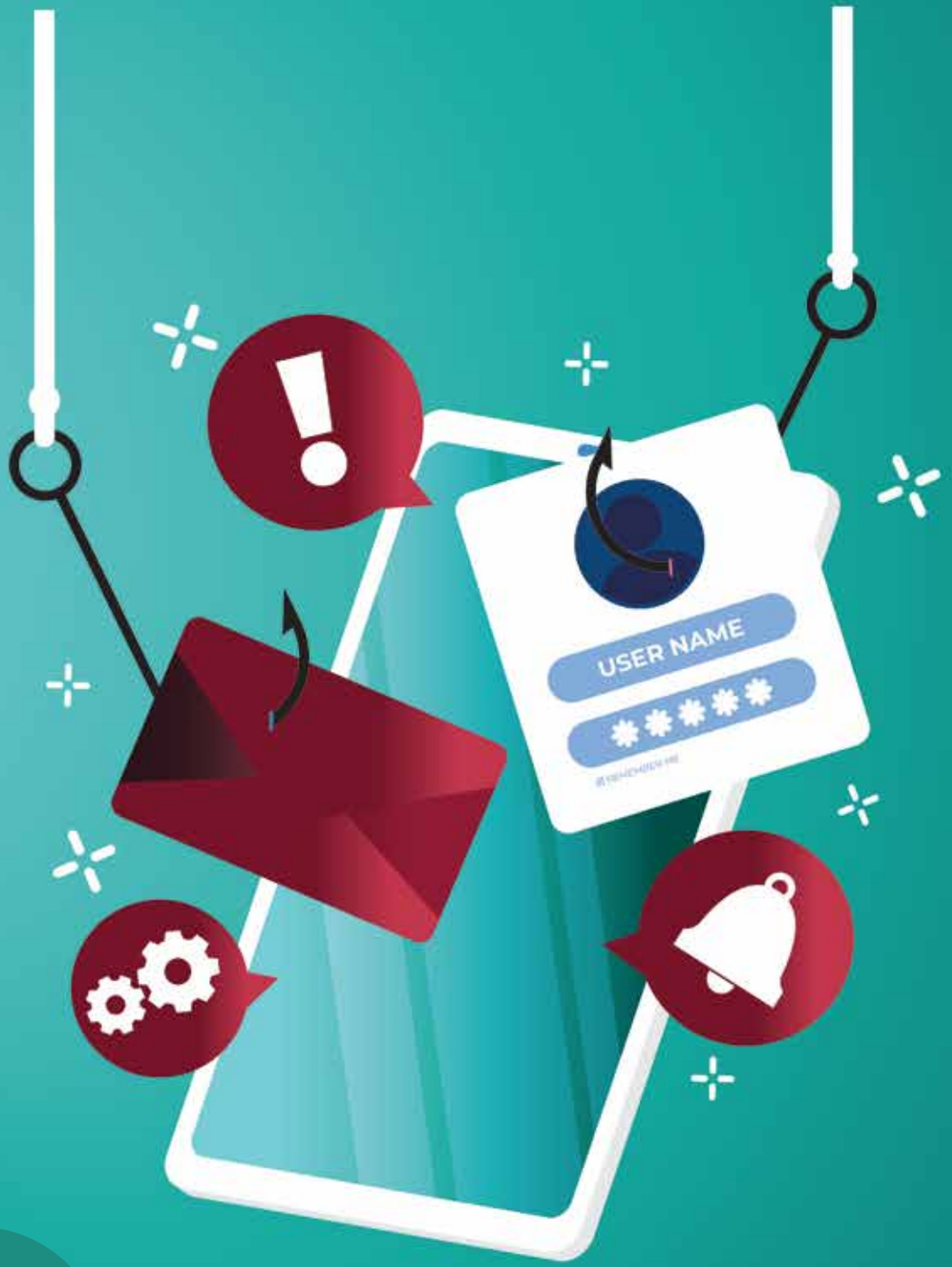
1. سرقة المعلومات أو الأموال من المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.
2. تثبيت البرمجيَّات الضَّارَّة على أجهزة المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.
3. تكون بوَّابة لتنفيذ عمليَّات أخرى لتخريب أنظمة المُؤسَّسَات المُسْتَهْدَفة.
4. دَفْع المُسْتَخْدِم الضَّحيَّة للدُّخول إلى موقع مُزيَّف على الإنترنت لإكمال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

- هجوم يتنكَّر فيه المُهاجِمون الإلكترونيّون في شخصيّة كيان معروف أو شخص حَسَن السُّمعة في رسالة بريد إلكترونيّ أو أيّ شَكْلٍ آخر من أشكال الاتّصال. **التَّصيُّد الاحتياليّ.**

- هو هجوم احتياليّ يَسْتهدِف فردًا ما داخل مؤسَّسة معيَّنة؛ بغرض سرقة بيانات اعتماد تسجيل الدُّخول الخاصَّة به. **التَّصيُّد الاحتياليّ المُوجَّه.**

- هو أحد أنواع هجمات التَّصَيُّد الاحتياليّ التي يتمّ تنفيذها عبر المكالمات الهاتفيَّة؛ بغرض الحصول على أموال الضَّحايا أو المعلومات الشَّخصيَّة الأخرى. **التَّصيُّد الصَّوْتيّ.**

- هو هجوم احتياليّ يتمّ عن طريق إرسال رسالة بريد إلكترونيّ إلى المُستخدِم المُستهدَف، تتضمَّن رابط موقع ويب مزيَّف، بهدف خداع الضَّحيَّة لإدخال معلوماته الخاصَّة. **التَّصيُّد الاحتياليّ عَبْر HTTPS.**

- هو هجوم يتسبَّب في ظهور رسائل احتياليَّة للمُستخدِمين في أثناء تصفُّحهم شبكة الإنترنت؛ حيث يُصيب المُهاجِمون مواقع الويب الأصليَّة ببرمجيَّات ضارَّة؛ ما يتسبَّب في ظهور هذه الرَّسائل المنبثقة عند زيارتها. **التَّصيُّد الاحتياليّ المُنْبَثِق.**

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

- 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. **التّصيُّد الموجّه لكبار الشّخصيّات.**

- هو هجوم احتياليّ يقوم فيه أحد المُتسلّلين بعمل نسخة مطابقة من الرّسالة التي استلمها المُستلِم بالفعل، وقد تتضمّن شيئًا مثل عبارة "إعادة إرسال هذا" ووَضع رابطٍ ضارٍّ في البريد الإلكترونيّ. **استنساخ التّصيُّد.**

- 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 رابطٍ معيّنٍ لكنّه في الحقيقة ضارٌّ؛ ما يتسبّب في إصابة أجهزة الحاسوب الخاصّة بهم. **التّصيُّد الخادع.**

أكمل الجمل التّالية

- يُعَدّ **التّصيُّد الاحتياليّ** إحدى الجَرائم الإلكترونيَّة الأكثر انتشارًا في العالَم.

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

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

- الهدف من هجمات التَّصَيُّد الاحتياليّ هو سرقة **المعلومات** أو **الأموال** من المُستخدِمين المُستهدَفين، و **تثبيت البرمجيّات الضَّارّة** على أجهزة المُستخدِمين، ودَفْع الضَّحِيَّة للدُّخول إلى **موقع مُزَيَّف** على الإنترنت.

- من طُرق المُهاجِمين الإلكترونيّين لخَرْق أجهزة المُستخدِمين المُستهدَفين إرسال **رسائل نصّيَّة** تحتوي على **رَوابِط** تتضمَّن **برمجيّات ضارّة** عند النَّقر عليها تسمح لـ **المُتَسلِّلين** بالتَّسلّل إلى جهاز الحاسوب.

- من علامات تعرّض الأجهزة الإلكترونيّة للخرق تلقّي إشعارات عبر البريد حول **التّصيّد الاحتياليّ المُنبَثِق** رغم عدم قيام المُستخدِم بذلك، **وبطء** الجهاز، وارتفاع **حرارته** ، وتأخّر الأوامر التي يتلقّاها من المُستخدِم.

- يُمثّل ظهور **نوافذ مُنبَثِقة** تحتوي على رسائل مزعجة تدّعي إصابة جهازك الإلكترونيّ بالفيروسات إحدى علامات تعرّض الجهاز للخرق.

- من الأخطاء التي يرتكبها مستخدمو الإنترنت: التّصفّح على شبكة **Wi-Fi عامّة** ، وعدم تحديث **نظام التّشغيل** و **التّطبيقات** الموجودة على الأجهزة، إلى جانب مشاركة كثير من **البيانات الشّخصيّة** على وسائل التّواصل الاجتماعيّ.

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

- من طُرق حماية البيانات من القرصنة: استخدام **البَصْمة الرّقميّة** ، فهي تُمثّل خطّ الدّفاع الأوّل ضدّ الهجمات الاحتياليّة.

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

1- من الأخطاء التي يقع فيها مَستخدِم 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. ✗
- مَشارَكة 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 البَصمَة 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 المَوجَّه:

- هجمات التَّصيُّد الاحْتِيَاليّ مَخصَّصة 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 واجب يقوم به الطَّالب بمفرده أو بالاشتراك مع زميل أو أكثر، ويقوم 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.

مراجـــــع

المحتوى العلمي

في الحـــــقيبة

1. 10 mistakes people make online. On site: https://cutt.us/4XQ7A
2. 10 Most Common Signs of a Phishing Email. On site: https://cutt.us/MJiQZ
3. 18 Ways to protect your data from hackers. On site: https://cutt.us/3M0uz
4. digital footprint. On site: https://cutt.us/P2gI8
5. How Does Clone Phishing Work? On site: https://cutt.us/x7Gwg
6. How to protect your digital footprint. On site: https://cutt.us/0ksRZ
7. How to Recognize and Avoid Phishing Scams. On site: https://cutt.us/0VwNx
8. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://cutt.us/20AV8
9. Importance of Digital Footprint: Complete Guide [2023]. On site: https://cutt.us/DCq7d
10. Phishing, Alexander S. Gillis, Technical Writer and Editor. On site: https://cutt.us/5jBhs
11. Scam Alert: What You Need to Know About Pop-Up Phishing. Onsite:https://cutt.us/3pHtA
12. Vishing – a growing threat. On site: https://cutt.us/q3aSU
13. Warning signs you've been hacked and what to do next. On site: https://cutt.us/rd84U
14. Whaling: how it works, and what your organization can do about it. On site: https://cutt.us/H9RNo
15. What is a digital footprint? And how to protect it from hackers. On site: https://cutt.us/bObsJ
16. What is an Evil Twin Attack? On site: https://cutt.us/jsBji
17. What Is Pharming and How to Protect Yourself. On site: https://cutt.us/BGtUI
18. What Is Phishing? On site: https://cutt.us/PbZ3Y
19. What is spear phishing? Definition and risks. On site: https://cutt.us/riHDD
20. What to Do If You Give Your Personal Information to a Phisher. On site: https://cutt.us/axv7k
21. Which 7 Online Mistakes Will You Make Today? On site: https://cutt.us/z25Nk

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency