CyberEco

مَعًا لِدَعْم السَّلامة الرَّقميّة
Together to support digital safety

هُجُوم التَّصيُّد الاحْتِيَالي

الحَقِيبَة التَّدريبيَّة

تَمارين وتَدْريبَات الطَّالب

المرحلة الإعداديَّة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

هُجُوم التَّصيُّد الاحْتِيَاليّ

الحقيبة التَّدريبيَّة / تمارين وتدريبات الطَّالب

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

عزيزي الطَّالب

هـذا الكُتَيِّـب خـاصٌّ بـكَ، ولا بُـدّ أن يكـون معـكَ عنـد حُضُـورك جلسـات التَّدْريـب، سـيقوم مُدَرِّبُـك بإرشـادك لكيفيَّـة اسـتخدامه. يحتـوي هـذا الكُتَيِّـب علـى مَجْمُوعـة مـن التَّمَاريـن المُمْتِعَـة والمُفِيـدَة، والتـي سـتقوم بالإجابـة عنهـا إمَّـا خـلال الصَّـفّ أو فـي منزلـك.

كمـا يحتـوي الكُتَيِّـب علـى مجموعـة مـن المُسـابَقَات والبطاقـات التَّعليميَّـة، والمعلومـات العَامَّـة، والتـي سـتجد فيهـا فائـدةً ومُتْعَـةً، وسيرشـدك المُـدَرِّب لكيفيَّـة التَّعامُـل مـع هـذه المُسـابَقات التَّدريبيَّـة، كمـا سَـنُزَوِّدك فـي مَطْلـع كُلّ تمريـن أو مُسـابَقة بتوجيهـات عامَّـة لكيفيَّـة الإجابـة.

السَّادة أولياء أمور الطَّلَبة

هذا الكُتَيِّب خاصّ بالطَّالب، وسيُرَافِقُه خلال التَّدْرِيب الَّذي سيتلقَّاه في المدرسة، وهو يحتوي على مجموعة من التَّمارين والتَّدريبات والمسابقات والبطاقات التَّدريبيَّة، والَّتي تتمحور جميعها حول المفاهيم ذات الصِّلة بالتَّصيُّد الاحتياليّ وكيفيَّة مواجهته.

الهدف من هذا الكُتَيِّب وما يحويه من تدريبات وأنشطة ذهنيَّة؛ تكريس وترسيخ المعلومات التي تَلقَّاها الطَّالب خلال محاضرة التَّدريب؛ وذلك لتحقيق هدفٍ رئيسٍ، يَتَمثَّل في تعزيز قدرة الطَّالب على استخدام الإنترنت والتِّكنولوجيا بفاعليَّة وأمان، وحمايته من مخاطر التَّصَيُّد الاحتياليّ وتدريبه على كيفيَّة التَّصرُّف في حال تعرُّضه لحوادث تَصَيُّد إلكترونيّ.

كلّ التَّمرينات والتَّدريبات الموجودة في الكُتَيِّب ستكون مرفقة بتوجيهات عامَّة لكيفيَّة الإجابة عنها، أمَّا المسابقات التَّدريبيَّة؛ فالمُدَرِّب هو مَن سيُقَدِّم للطَّالِب توجيهات حلِّها، كما أنَّ الكُتَيِّب يحتوي على بعض التَّدريبات والتَّمارين اللاصفِّيَّة، وهذه التَّمارين سيقوم بالإجابة عنها بالمنزل، وهي الأخرى ستكون مرفقة بتوجيهات للحلّ.

يُرْجَى منكم الإشراف غير المباشر على الطَّالب خلال تَعامُله مع الكتاب، وفي حال تَوَجَّه الطَّالب إليكم بسؤال أو استفسار حول أحد التَّمارين أو التَّدريبات، فيُرْجَى قراءة التَّوجيهات الخاصَّة بكلّ تمرين، وتقديم العون للطَّالب في ضوء هذه التَّوجيهات.

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 «الخطأ» فيما يتعلّق بالتَّصَيُّد الاحتياليّ:

تَوْجيه

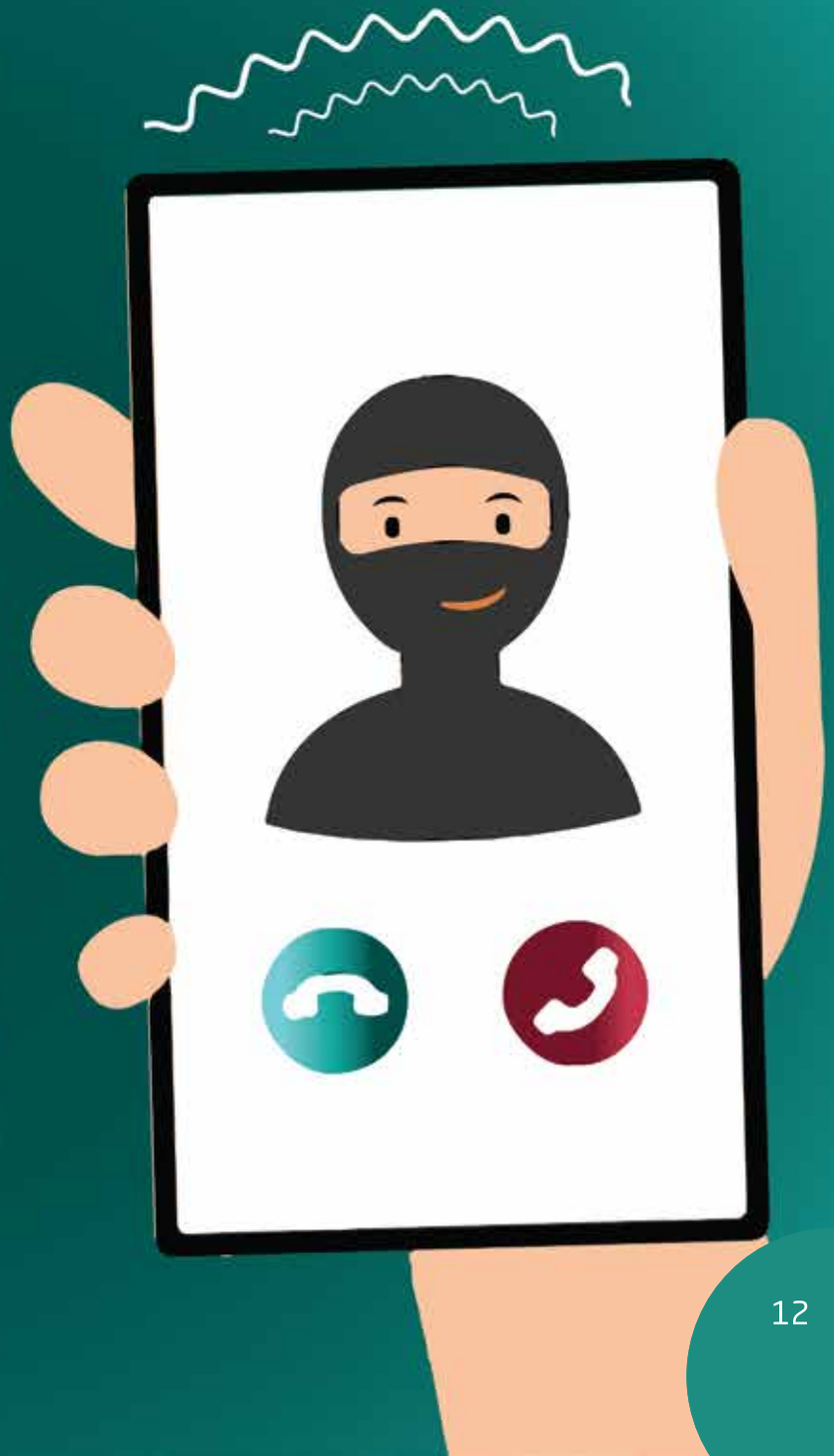
اقْرأ العبارات الواردة بتَمَعُّن، وفكِّر فيما إذا كانت هذه العبارات تُعبّر عن معلومات صحيحة أو خاطئة فيما يَتعلّق بالتَّصَيُّد الاحتياليّ، ثمّ وَضْع مثال محلول في الجدول.

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



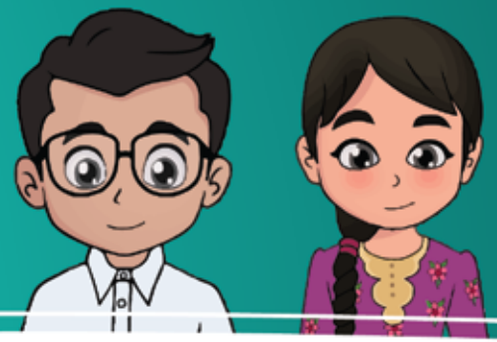
انْتَبِه!

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

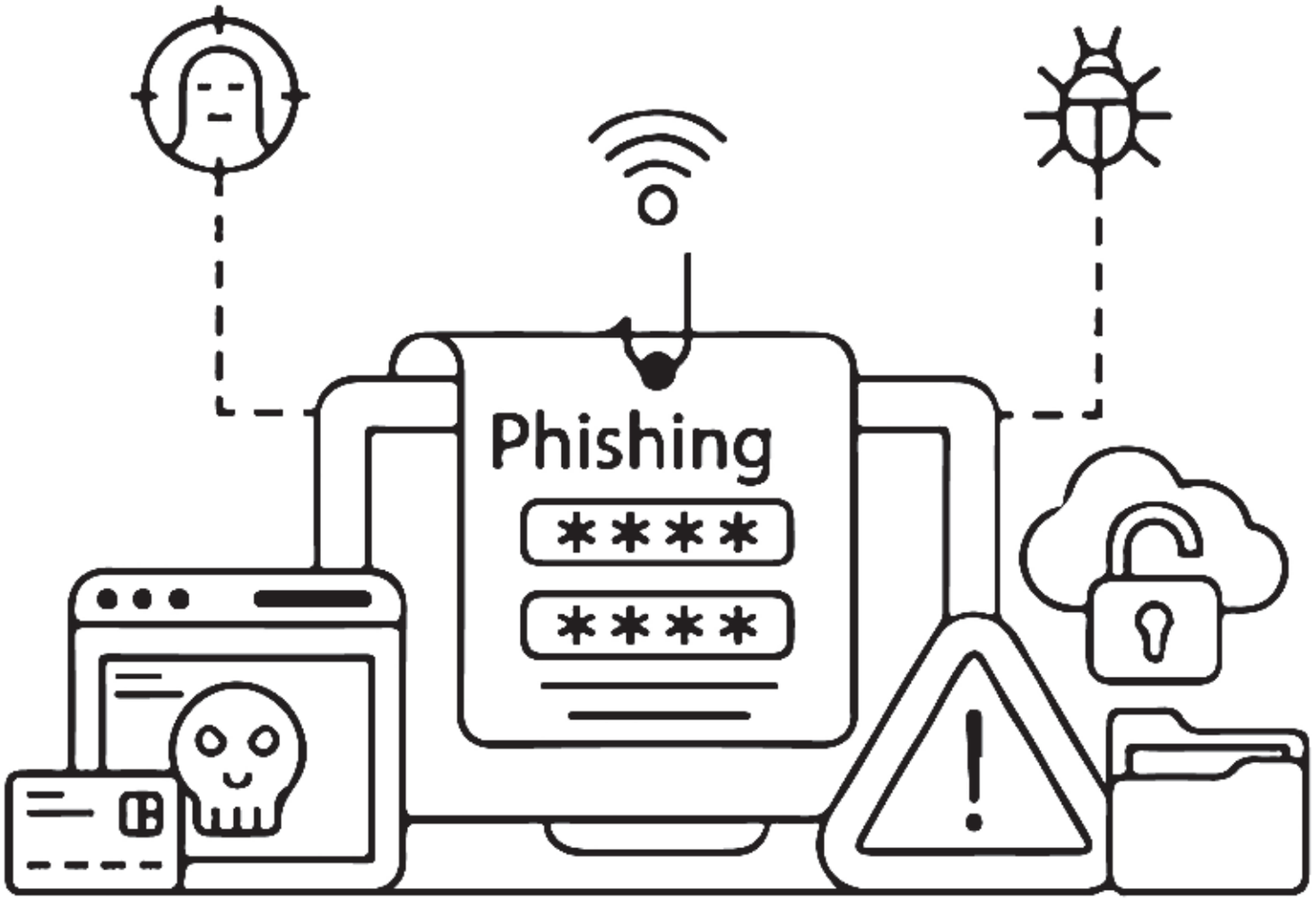
ضَع الكلمة المناسبة لكلّ تعريف



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 مَرْفق من المَرْفقات 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 الاحْتِيَالِيّ عَبْر HTTPS

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

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

رتِّب العِبارات التَّالية وفقًا للتَّسلسل المنطقيّ...

كيفَ تحمي نفسك من التصيد الاحتيالي؟

توجيه

اقرأ الجُمَل الواردة في الجدول بتَمَعُّن، وأعِد ترتيب الجُمَل بحيثُ تكون الجُمْلَة الأُولَى تُعَبِّر عن التَّصرُّف الأوَّل الَّذي يجب أنْ تتصرَّفه فور تَعَرُّضِك للتصيد الاحتيالي، والجُمْلَة الثَّانية هي التَّصرُّف الثَّاني، وهكذا.

1	في حالة استخدام اسم شركة أو موقع، عليك التَّواصل مع الشَّركة وتحذيرها من استخدام اسمها في أعمال وأغراض احتياليَّة.	
2	توجَّه فورًا إلى وحدة الجرائم الإلكترونية بوزارة الداخلية للإبلاغ عمَّا حدث معك خاصَّةً في حالة سرقة الأموال.	
3	في حال تمّ سرقة بيانات حساباتك البنكيَّة أو البطاقات الائتمانيَّة؛ تواصل مع البنك فورًا لوقف أيّ تعاملات على حسابك.	
4	عليك كتابة منشورات تشرح فيها كيف تَعرَّضْت للتَّصَيُّد الاحتياليّ كيلا يقع غيرك في الفَخّ نفسه.	
5	أَوقِفْ جميع أنواع التَّواصل مع هذا المَحتال الذي حاول أن يَخْدَعَك.	
6	في حالة كان التَّصَيُّد من خلال إعلان لوظيفة ما، عليك الإبلاغ فورًا عن الإعلان المشبوه.	
7	إن كنت تعتقد أنّ حاسوبك أو هاتفك تعرَّض للخرق، فعليك أن تُوقِف اتِّصاله بالإنترنت فورًا وأن تذهب لمتُخصِّص لمساعدتك من أجل تأمين جهازك ووَضْع برامج للحماية.	

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 السِّرِّيّة الخاصّة بك عبر الهاتف، سواء للأسرة أم للجِهات المسؤولة.
4. مُشارَكة كثير من المعلومات الشَّخصيّة عبر منصّات 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 تَدَّعي 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 الاحْتِيَاليّ؛ حيث يتمّ تصميم موقع ويب مُزيَّف، ثم إعادة توجيه المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ إليه لسرقة المعلومات السِّرِّيَّة.

التَّمرين السَّادس

عمليّات الشّراء الإلكترونيّة.	
التّسجيل في المواقع الإلكترونيّة.	
تحميل التّطبيقات من مَتاجِر التّطبيقات.	
التّحدُّث عبر الهاتف.	
التّسجيل في النّشرات العامّة.	
الذّهاب في نزهة.	
بيع وشراء الأسهم.	
الاشتراك في المجلّات الإلكترونيّة.	
فتح حساب بنكيّ.	
منشورات منصّات التّواصل الاجتماعيّ.	
مشاهدة برامج على التّلفاز.	
مشاركة المعلومات والصُّور مع الأصدقاء.	
إعادة نَشْر المقالات والمعلومات التي تقرأها.	
الاشتراك في المُدوّنات الصّحّيّة.	
نَشْر المقاطع المُصَوَّرة عبر منصّات التّواصل 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, يتسـبَّب فـي إصـابة 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 الاحْتيَالي 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 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 الأوّل

استخرج الكلمات التّالية من الجدول:

توجيه

اقرأ الكلمات الواردة أدناه بتمعّن، وابحث في الجدول عن حروف متتالية تُشكّل 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 مُطابِقة 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 عبر بريدك الإلكترونيّ حقيقيّة أم مجرّد تصيُّدٍ احتياليّ؟ وكيف ستتصرّف حيالها؟

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؟

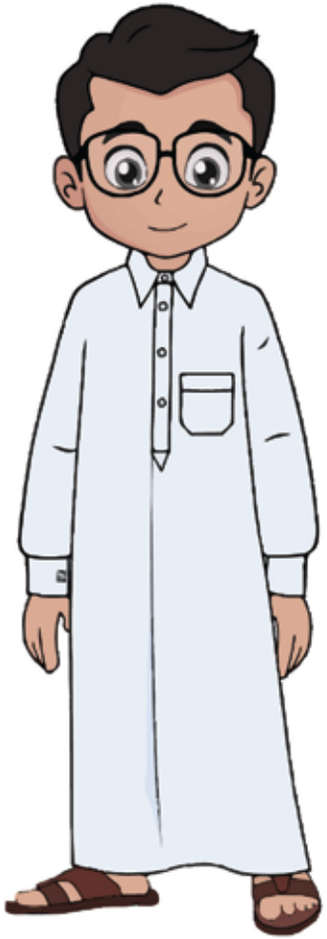

01001110
01110100
0111011101
111100010110

التَّمرين الرَّابع

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

تحقَّق من المُرسِل، 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 لمزوّدي 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



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

التّمرين السّادس

عَـــــــرِّف المصطلحات التّـــــالية

الهندسة الاجتماعيَّة .....

كلمة المرور .....

التَّصَيُّد الاحتياليّ .....

البَصْمة الرَّقميَّة .....

الاحتيال عبر الإنترنت .....

أهداف هجمات التَّصيُّد الاحْتِيَالِيّ

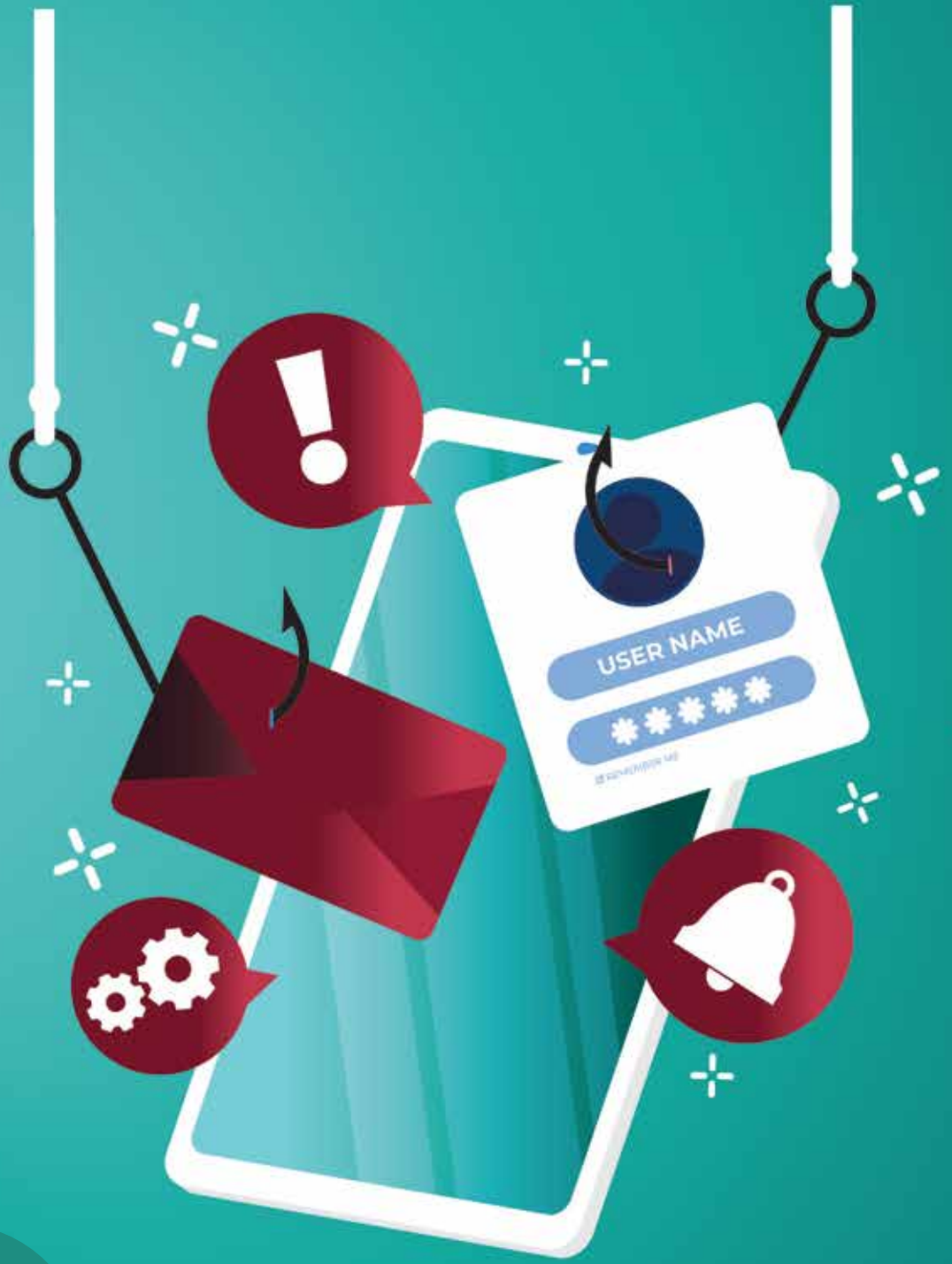
1. سرقة المعلومات أو الأموال من المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.
2. تثبيت البرمجيَّات الضَّارَّة على أجهزة المُسْتَخْدِمِينَ المُسْتَهْدَفِينَ.
3. تكون بوَّابة لتنفيذ عمليَّات أخرى لتخريب أنظمة المُؤسَّسَات المُسْتَهْدَفة.
4. دَفْع المُسْتَخْدِم الضَّحيَّة للدُّخول إلى موقع مُزيَّف على الإنترنت لإكمال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

علامات تُمَيِّز الرَّسَائل البريديَّة التَّصيُّديَّة

1. أسلوب الكتابة غير المألوف للمُستقبِل.
2. الأخطاء النّحويَّة والإملائيَّة.
3. التَّناقُض في عناوين البريد الإلكترونيّ والرَّوابِط.
4. الإلحاح وإثارة مَشاعر الخوف.
5. المُرفَقات 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 المُسمَّى المُناسِب

- هو هجوم عبر الإنترنت يعمل على خداع المُستهدَفين للاتِّصال بشبكة Wi-Fi مزيَّفة تُشبه الأصليَّة، وعند الاتِّصال يبدأ المُهاجِم التَّسلُّل إلى الأجهزة الخاصَّة بالضَّحايا لسرقة كلّ ما عليها من بيانات وملفَّات.

- هو هجوم احتياليّ يَستهدِف كبار المسؤولين التَّنفيذيِّين في المؤسَّسات العالميَّة، ويأتي متنكِّرًا في صورة رسالة بريد إلكترونيّ مألوفة، وهو مصمَّم على تحفيز ضحاياه على القيام بإجراءات مثل تحويل الأموال أو إرسال بيانات شخصيَّة.

- هو هجوم احتياليّ يقوم فيه أحد المُتسلِّلين بعمل نسخة مطابقة من الرِّسالة التي استلمها المُستلِم بالفعل، وقد تتضمَّن شيئًا مثل عبارة "إعادة إرسال هذا" ووَضْع رابطٍ ضارٍّ في البريد الإلكترونيّ.

- هو هجوم احتياليّ يَستخدِم فيه المُهاجِم تقنيَّة خادعة للتَّظاهر بأنَّه يعمل مع شركة حقيقيَّة لإبلاغ المُستخدِمين المُستهدَفين بأنَّهم يتعرَّضون بالفعل لهجوم إلكترونيّ، لدفعهم للنَّقر على رابطٍ معيَّنٍ لكنَّه في الحقيقة ضارٌّ؛ ما يتسبَّب في إصابة أجهزة الحاسوب الخاصَّة بهم.

- هجوم يتنكَّر فيه المُهاجِمون الإلكترونيُّون في شخصيَّة كيان معروف أو شخص حَسَن السُّمعة في رسالة بريد إلكترونيّ أو أيّ شَكْلٍ آخر من أشكال الاتِّصال.
- هو هجوم احتياليّ يَسْتهدِف فردًا ما داخل مؤسَّسة معيَّنة؛ بغرض سرقة بيانات اعتماد تسجيل الدُّخول الخاصَّة به.
- هو أحد أنواع هجمات التَّصَيُّد الاحتياليّ التي يتمّ تنفيذها عبر المكالمات الهاتفيَّة؛ بغرض الحصول على أموال الضَّحايا أو المعلومات الشَّخصيَّة الأخرى.
- هو هجوم احتياليّ يتمّ عن طريق إرسال رسالة بريد إلكترونيّ إلى المُستخدِم المُستهدَف، تتضمَّن رابط موقع ويب مزيَّف، بهدف خداع الضَّحِيَّة لإدخال معلوماته الخاصَّة.
- 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.

أكمل الجمل التّالية

- يُعَدّ ..... إحدى الجَرائم 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 ..... تتضمَّن ..... عند النَّقر عليها تسمح لـ ..... بالتَّسلّل إلى جهاز الحاسوب.

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

- 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.

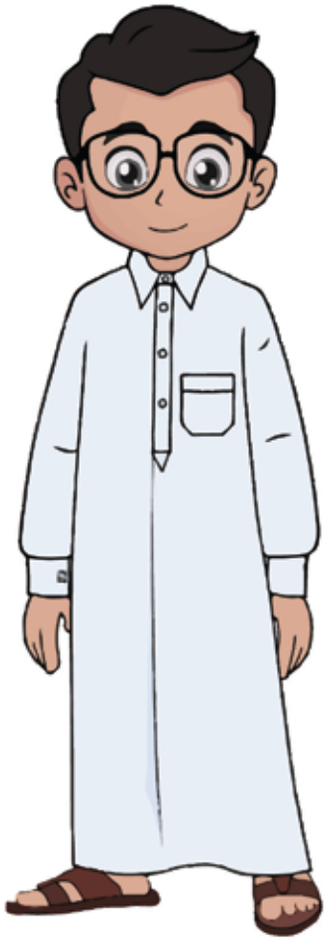
- ..... هي مسار البيانات التي يتركها المَستخدِم عند استخدام شبكة الإنترنت.

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

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

1- من الأخطاء التي يقع فيها مُستخدِم الإنترنت خلال أداء مَهامّه أو التَّصفُّح على الشبكة العالميَّة:

- التَّصفُّح على شبكة Wi-Fi العامَّة دون اتِّخاذ الاحتياطيات الأمنيَّة. ○
- تحديث المُتصفِّح والتَّطبيقات الموجودة على الأجهزة. ○
- مُشارَكة الكثير من المعلومات الشَّخصيَّة على وسائل التَّواصُل الاجْتِمَاعيّ. ○
- اختلاف كلمات المرور لعددٍ من الحسابات الشَّخصيَّة للمُستخدِم عبر الإنترنت. ○
- تثبيت تحديثات البرنامج تلقائيًّا. ○
- فتح الرَّوابِط من رسائل البريد الإلكترونيّ دون التَّحقُّق من موثوقيتها. ○
- عدم الاستفادة من إعدادات الخصوصيَّة الخاصَّة بك على وسائل التَّواصُل الاجْتِمَاعيّ. ○



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.

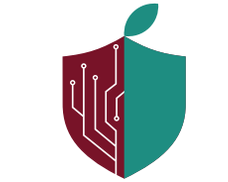
3- الفرق بين التَّصيُّد الاخْتِيَاليّ والتَّصيُّد الاخْتِيَاليّ المَوجَّه:

- هجمات التَّصيُّد الاخْتِيَاليّ 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 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.



CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency