



حقوق الملكية الفكرية

الدليل مملوك للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافة حقوق الملكية الفكرية التي تشمل حق المؤلف وحقوق التأليف والنشر والطباعة، كلها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر. وعليه فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي أجزاء من هذا الدليل، أو الاقتباس منه، أو نسخ أي جزء منه، أو نقله كلياً أو جزئياً في أي شكل وبأي وسيلة، سواءً بطرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نظم تخزين المعلومات واسترجاعها سواءً من الأنظمة الحالية أو المبتكرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذن خطي منها. ومن يخالف ذلك يُعرض نفسه للمساءلة القانونية.

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدارة التميز السيبراني الوطني، الوكالة الوطنية للأمن السيبراني.

للاستفسار عن المبادرة أو البرنامج، يمكن التواصل عن طريق المواقع الإلكترونية أو الأرقام الهاتفية التالية:



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ cyberexcellence@ncsa.gov.qa

☎ 00974 404 663 78

☎ 00974 404 663 62

الفهرس

07	مَن نحن؟
09	تمهيد
11	فكرة الدليل
11	أهمية الدليل
12	أهداف الدليل
13	دور المُدرِّب تجاه الطلّبة في الألعاب التّدرّبيّة
14	تصور عامّ للألعاب التّدرّبيّة
17	اللّعبة الأولى: Cyber Block
19	• أهداف اللّعبة
19	• السنّ المناسبة للّعبة
20	• مكوّنات اللّعبة
26	• آليّة اللّعب
29	اللّعبة الثّانية: Cyber Quiz
31	• أهداف اللّعبة
31	• السنّ المناسبة للّعبة
32	• مكوّنات اللّعبة
33	• آليّة اللّعب
34	• موضوعات البطاقات السيبرانيّة وأسئلتها

49		اللَّعْبَةُ الثَّالِثَةُ: Cyberno
51		• أهداف اللَّعْبَةِ
51		• السَّنُ الْمُنَاسِبَةُ لِلَّعْبَةِ
52		• مُكَوِّنَاتُ اللَّعْبَةِ
64		• طَرِيقَةُ اللَّعْبِ
65		• قَوَانِينُ اللَّعْبَةِ
67		اللَّعْبَةُ الرَّابِعَةُ: Cyber Way
69		• فِكْرَةُ اللَّعْبَةِ
69		• السَّنُ الْمُنَاسِبَةُ لِلَّعْبَةِ
69		• تَسْمِيَةُ اللَّعْبَةِ
70		• النِّقَاطُ الْمُمَيِّزَةُ فِي اللَّعْبَةِ
70		• مُكَوِّنَاتُ اللَّعْبَةِ
71		• أَنْوَاعُ الْمُرَبَّعَاتِ
72		• طَرِيقَةُ اللَّعْبَةِ

75		اللَّعْبَةُ الْخَامِسَةُ: لعبة الأفكار التَّعليمِيَّة
77		• فِكْرَةُ اللَّعْبَةِ
77		• السَّنْ الْمُنَاسِبَةُ لِلْعَبَةِ
77		• أَهْدَافُ اللَّعْبَةِ
77		• مُكَوِّنَاتُ اللَّعْبَةِ
78		• آليَّةُ اللَّعِبِ
80		أَسْأَلُ تَقْيِيمِ أَدَاءِ الطَّلَبَةِ فِي الْأَلْعَابِ التَّدْرِيبِيَّةِ





مَنْ نحن؟

الوكالة الوطنية للأمن السيبراني
مؤسسة وطنية تُعنى بتطوير وحماية الفضاء السيبراني في دولة قطر، وتعزيز
كفاءة وفاعلية البيئة الرقمية، بما يدعم تطور الدولة والمجتمع، ويسهم في
تحقيق رؤية قطر 2030.



تمهيد

تُعَدُّ الألعاب التَّدرِيبِيَّة أداة فعَّالة في التَّدرِيب، لا سيَّما على مستوى الأطفال والبالغين، فهي تجمع ما بين التَّدرِيب والتَّسْلِيَة، ما يُحَفِّز الطَّلَبَة على الاندماج في اللُّعْبَة والحصول على المعلومات، كما تُعَدُّ إحدى أدوات التَّدرِيب التَّفَاعُلِي الأكثر فاعليَّة، خاصَّةً إذا كانت ألعابًا جماعيَّة؛ فالألعاب الجماعيَّة لها قُدْرَة عالية على تحفيز التَّفَاعُل المعرفي والتَّفَانُسي بين الطَّلَبَة، وهو ما يَدْعِم تحقيق هدف اللُّعْبَة الرِّئيس، والمُتمثِّل بتقديم معلومات للطَّلَبَة ضَمَّن إطار من التَّفَانُس والتَّسْلِيَة.

في إطار الأدوات التَّدرِيبِيَّة التي يَعمَدُها مشروع الزِّيَارَات المَبْدِئِيَّة للمدارس الحكوميَّة والخاصَّة في دولة قطر؛ تمَّ اعتماد الألعاب التَّدرِيبِيَّة أداةً رئيسةً، وهذه الألعاب ستتمَّ بإشراف غير مُباشر من المُدرِّبين، ولَدْعَم قُدْرَة المُدرِّبين على توجيه الطَّلَبَة لكيفيَّة التَّفَاعُل مع هذه الألعاب، وكيفيَّة تقييم أدائهم، لا بُدَّ من تزويدهم بِدَلِيل إجرائيٍّ يُقَدِّم لهم المعلومات اللازمَة حول الألعاب المُعْتَمَدَة، وتقديم معلومات تفصيليَّة حول كُلِّ لُّعْبَة، وآليَّات التَّقييم المُقْتَرَحَة.





فكرة الدليل

تقوم فكرة الدليل على ضرورة تقديم الدعم المعرفي اللازم للمدربين للتعامل مع الألعاب التدريبية، وتقديم شرح تفصيلي حول كل لعبة؛ بحيث يتمكن المدرب من شرحها للطلبة، كما تشمل الفكرة تزويد المدربين بمنهجية تقييم أداء الطلبة في الألعاب؛ فعند لعب الطلبة بالألعاب التدريبية لا بد للمدرب من تقييم أدائهم، لا سيما الأداء المعرفي، وملاحظة قدرتهم على استخدام المعلومات التي تم تدريبهم عليها في الألعاب؛ فالألعاب بمجملها تعتمد على قدرة الطالب على استخدام المعلومات والمعارف التي تم تزويده بها في الألعاب، ومعيار الفوز في الألعاب يعتمد بشكل رئيس على المخزون المعرفي لدى الطلبة، فكلما كان لدى الطالب مخزون معرفي رقمي أكبر، ارتفعت قدرته على الفوز في الألعاب.

أهمية الدليل

يستمد الدليل أهميته من أهمية الألعاب التدريبية، ودورها في دعم وتعزيز المخزون المعرفي الرقمي لدى الطلبة، ودورها في تقييم أداء الطلبة وتقييم قدرتهم على استثمار المعلومات والمفاهيم التي تم تدريبهم عليها، وفيما يلي تبيان لأبرز النقاط التي توضح أهمية الدليل:

- ضرورة تزويد المدربين بمعلومات تفصيلية حول كل لعبة من الألعاب التدريبية، بما يمكنهم من توجيه الطلبة لكيفية اللعب.
- ضرورة تزويد المدربين بمنهجية تقييم أداء الطلبة في الألعاب التدريبية.
- أهمية ملاحظة وتقييم قدرة الطلبة على استثمار مخزونهم المعرفي الرقمي في الألعاب.

- يهدف دليل المُدَرِّب للألعاب التَّدرِيبِيَّة لِتَحْقِيقِ الأَهْدَافِ التَّالِيَةِ:
- تَعْزِيزُ قُدْرَةِ المُدَرِّبِينَ عَلَى التَّعَامُلِ مَعَ الألعابِ التَّدرِيبِيَّةِ، وَتَعْزِيزُ قُدْرَتِهِمْ عَلَى تَوْجِيهِ الطَّلَبَةِ لِكَيْفِيَّةِ اللَّعِبِ.
- تَزْوِيدُ المُدَرِّبِينَ بِمَعْلُومَاتٍ تَفْصِيلِيَّةٍ عَنِ كُلِّ لُعْبَةٍ، وَتَحْدِيدُ أَهْدَافِهَا وَطَرِيقَةِ لَعِبِهَا.
- تَزْوِيدُ المُدَرِّبِينَ بِمَنْهَجِيَّةٍ وَاضِحَةٍ لِتَقْيِيمِ أَدَاءِ الطَّلَبَةِ فِي الألعابِ التَّدرِيبِيَّةِ، وَكَيْفِيَّةِ تَقْيِيمِ قُدْرَةِ الطَّلَبَةِ عَلَى اسْتِثْمَارِ مَخَزُونِهِمِ المَعْرِفِيِّ لِلقَّوْزِ فِي الألعابِ.





دور المُدرِّب تجاه الطَّلَبَة في الألعاب التَّدرِيبِيَّة

لتحقيق الألعاب التَّدرِيبِيَّة الأهداف المُناطَة بها، على المُدرِّب أن يقوم بقَدَرٍ

من المهام والواجبات، فيما يلي تبيان لأهمِّها:

- الإشراف على توزيع الطَّلَبَة على الألعاب التَّدرِيبِيَّة، والإشراف غير المُباشر على تشكُّل الفِرَق، في حال كانت اللُّعْبَة جماعيَّة.
- توضيح آليَّة اللُّعْب للطلَّبة، وشرح أهداف اللُّعْب وطريقة لعبها.
- الإجابة عن استفسارات الطَّلَبَة فيما يتعلَّق بالألعاب وقوانينها.
- الإشراف المُباشر على اللُّعْبَة، وتسجيل الملاحظات حول أداء الطَّلَبَة، لاستخدام هذه المُلاحظات في التَّقييم.

تَصَوُّر عامٌ للألعاب التَّدرِيبِيَّة

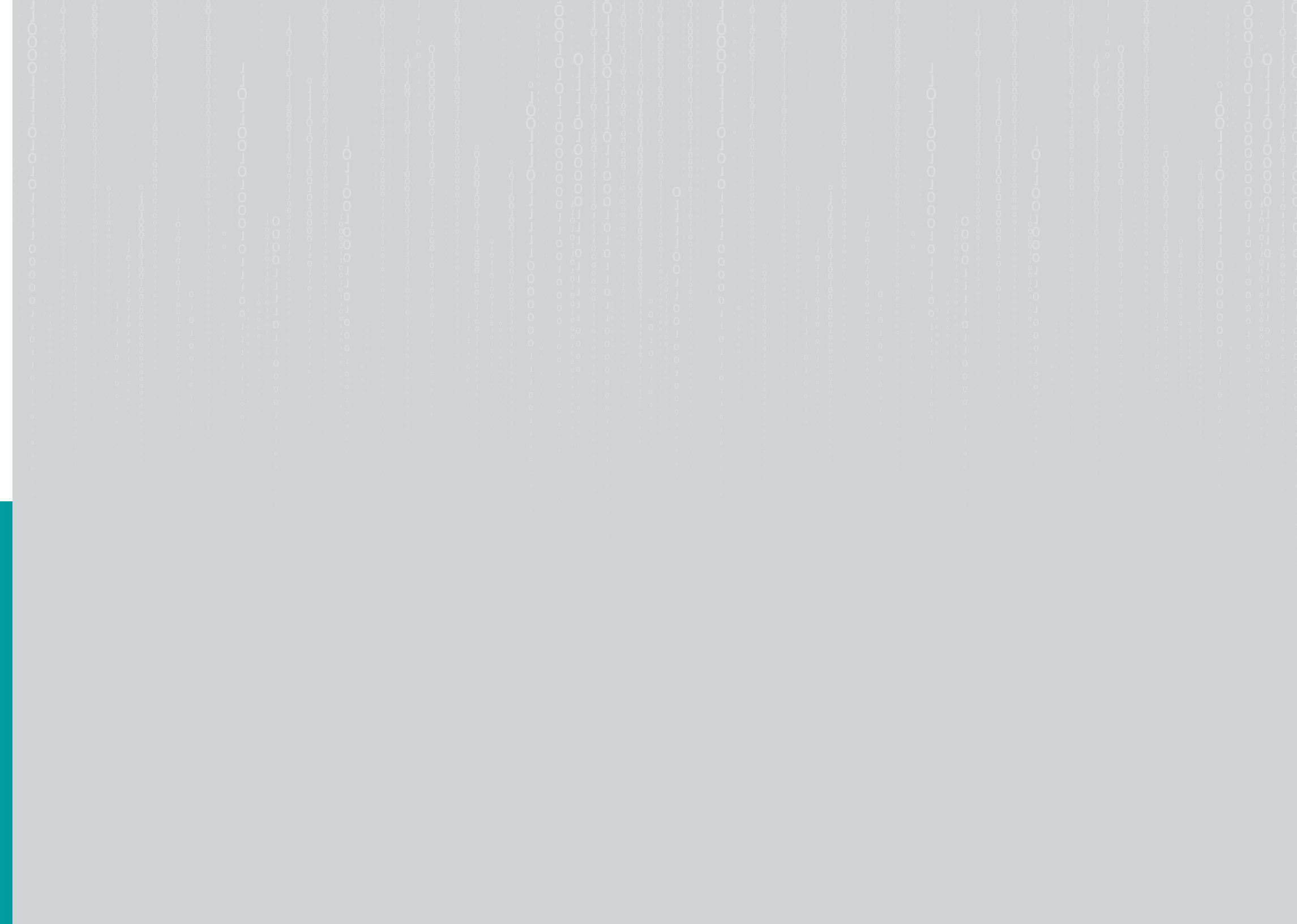
يبلغ عدد الألعاب خمس ألعاب تدرِيبِيَّة، مختلفة في شَكْلِها العام وفي طريقة لعبها، ومُشتركة في نقطة رئيسة، وهي أنَّ القَوَز بها يَعمَد بشكلٍ رئيسٍ على المخزون المعرفي الرَّقميِّ للطَّالب، كما تختلف الألعاب فيما بينها وفقًا لعدد الطلبة في كُلِّ لُعبَةٍ، وتبعا للسنِّ المُخصَّصة لكلِّ منها. وبشكلٍ عامٍّ؛ فإنَّ الألعاب بمُجملها تُغطِّي مُختلف الأعمار في المراحل التَّعليميَّة الثلاث؛ الابتدائيَّة والإعداديَّة والثَّانويَّة، وفي الجدول التالي تبيان للأعمار المُخصَّصة لكلِّ لُعبَةٍ، ولعدد الطلبة.





اللَّعْبَة	Cyber Block	Cyber Quiz	Cyberno	Cyber Way	لعبة الأفكار التعليمية
السِّن	10+ سنوات	7+ سنوات	17+ سنة	15+ سنة	4-6 سنوات
عدد الطلّبة	فريقان وحكم، كلّ فريق يتكوّن من طالب أو طالبين	فريقان وحكم، كلّ فريق يتكوّن من طالب واحد وحتى 5 طلبة.	2 - 6 طلبة مع حكم.	ثلاثة فرق، كلّ فريق بين 1 - 3 طلبة.	طالبان أو أكثر
معيّار الفوز	الفريق الفائز هو الحاصل على أكبر عدد من النقاط (Coins)	الطالب الفائز هو الحاصل على أكبر عدد ممكن من النقاط (Coins)	الطالب الذي ينتهي من جميع بطاقاته أولاً هو الفائز	الفريق الواصل أولاً للمربع رقم 100 هو الفائز.	الطالب الفائز هو الذي استطاع الفوز بأكثر دورات اللعبة عدداً.

وفيما يلي تبيان لتفاصيل الألعاب وكيفية لعبها وأهدافها وقواعدها.





اللّعبة الأولى: Cyber Block



"Cyber Block" هي لعبة تُقدّم أفكارًا ومعارف أساسية مُرتبطة بالأمن السيبراني، وما يتعلّق به من موضوعات مُهمّة بشكلٍ مُبسّطٍ ومُسلٍّ للطلّبة واليافعين؛ بما يُساعد الطّلبة على التّعلّم بطريقةٍ مُبتكرةٍ وغير تقليديّة.

أهداف اللّعبة

- تنمية المهارات الرّقمية للطلّبة.
- تعريف الطّلبة بمفاهيم ومُصطلحات سيبرانيّة جديدة.
- تبسيط المعلّومات وإيصالها للطلّبة بطريقة مُسليّة.
- إيصال المعلّومات الخاصّة بالأمن السيبرانيّ بطريقة مُسليّة تُساعد على الإدراك التّام لهذه المعلّومات.
- كتابة المُصطلحات باللّغتين العربيّة والإنجليزيّة يُعزّز من قُدرة الطّلبة على التّعامل الفعّال مع البيئة السيبرانيّة.
- تحفيز الطّلبة وتعزيز شُعورهم بالحماس والتّسلية والإنجاز عن طريق جَمع أكبر قدر مُمكن من الجوائز وهزيمة المُنافسين.

السنّ المناسبة للّعبة

10+ سنوات

مُكوّنات اللعبة

1. لوح كبير مقسم إلى 24 محطة، بلوّين:

• 12 محطة باللون الأخضر (المحطات الآمنة سيرانيًا)؛ تضم مصطلحات

إيجابية في الأمن السيراني، وهي:

1. السريّة confidentiality

وهي التحكم في الدّخول إلى البيانات وإتاحتها أو السماح بالدّخول فيها لفئات مُعيّنة.

2. السّلامة integrity

الحفاظ على سلامة البيانات والمعلومات، وكذلك حمايتها من الهجمات التخريبية أو السرقة.

3. التّوافر Availability

جاهزية جميع الأنظمة والخدمات والمعلومات، وكذلك إتاحتها حسب طلب الشّركات أو العملاء.

4. أمن الشّبكات Network security

ممارسة تأمين شبكة الحاسوب من المُتطفّلين من خلال تكنولوجيا البرامج والأجهزة المختلفة، وتشمل جدار الحماية، وأمان البريد الإلكتروني، وبرامج مكافحة الفيروسات والبرمجيات الضّارة.

5. أمن المعلومات Information security

عملية تصميم ونشر أدوات من أجل حماية المعلومات المُهمّة من التّلف أو الضّيع أو التّعديل أو التّعطل، خاصّة في حالة النّقل أو التّخزين، ويشمل التّشفير وإدارة نقاط الضّعف.

6. أمن التطبيقات Application security

يُركّز على إبقاء البرامج والأجهزة خالية من أيّ تهديدات، وتتمّ تلك المرحلة عادةً في أثناء مرحلة التصميم، وقبل عملية نشر البرنامج أو الجهاز بوقتٍ طويل.

7. الأمن التشغيلي Operational Security

هو عملية إدارة المخاطر لجميع عمليّات الأمن السيراني الداخليّة، ويشمل العمليّات والقرارات الخاصّة بمعالجة أصول البيانات وحمايتها، بما في ذلك أذون الدّخول وإجراءات تخزين البيانات والمُشارَكة.

8. الأمن السحابي Cloud security

يتضمن حماية أنظمة التخزين السحابية الأساسية في كل الأوقات؛ لما عليها من كميات هائلة من البيانات، ويتضمن أيضاً خدمات الأعمال المخزنة في مركز البيانات.

9. أمن البنية التحتية Infrastructure security

هو إجراء أمني يحمي البنية التحتية الحيوية، مثل أنظمة الاتصالات أو الشبكات، أو مراكز البيانات والخوادم أو مراكز تكنولوجيا المعلومات من أجل حمايتها من العمليات الإرهابية أو محاولات الإفساد والتخريب.

10. الردع السيبراني Cyber Deterrence

هو كل ما يتعلق بمنع الأعمال الضارة والهجمات التي قد تحدث في الفضاء السيبراني.

11. الهاكر الأخلاقي Hacker, White Hat

هو شخص أو مجموعة من الأشخاص يقومون بمحاولة شرعية لاختراق النظام الخاص بالمؤسسة/الشركة؛ لكشف نقاط الضعف التي يمكن لمهاجم (هاكر غير أخلاقي) أن يقوم باستغلالها للوصول غير الشرعي إلى النظام/البيانات.

12. مُصادقة هوية المُستخدم User Authentication

هي تقنية تمنع المستخدمين غير المصرح لهم من الوصول إلى مستوى معين من المعلومات، وتحديد المستخدمين الذين يُمكنهم الوصول إلى هذا المستوى.



- 12 محطة باللون الأحمر (المحطات الخطرة سيبرانيًا)؛ تضم مصطلحات سلبية تُشكل خطرًا سيبرانيًا مُعيّنًا، وهي:

1. الهجمات الإلكترونية Cyber-Attacks هي أي هجوم يحاول التّحكم أو التّعديل أو التّغيير أو إفساد أو تعطيل أو تدمير أو السرقة في الفضاء الإلكتروني، وغالبًا ما تستهدف المؤسسات من أجل تدميرها أو الإضرار بها وبسلامة البيانات والمعلومات التي تحتوي عليها.

2. الجريمة الإلكترونية Cybercrime هي شكل مُتطور من الجريمة، وتحدث على نطاق عالمي، وتستهدف الحواسيب أو الشبكات أو البنى التحتية.

3. هجمات التّصيد الاحتيالي Phishing Attacks هي نوع من الهجمات يهدف إلى سرقة أو إتلاف البيانات الحساسة؛ من خلال خداع الأشخاص للحصول على بياناتهم الشخصية والتّحكم بها، وغالبًا ما تستهدف البيانات البنكية أو كلمات المرور.

4. هجمات التّصيد الاحتيالي المُوجّه Spear Phishing Attacks وهو عملية احتيال تتم من خلال البريد الإلكتروني أو الاتصالات الإلكترونية، وتستهدف الأفراد أو المنظمات أو الشركات، والهدف الأساسي منها سرقة البيانات، وغالبًا ما تعتمد على تثبيت برمجيات ضارة على جهاز الضحية.

5. هجمات التّشفير Encryption Attacks

هذه الهجمات هي عبارة عن برنامج نصي ضار يقوم بتحميل نفسه تلقائيًا، ويثبت نفسه على جهاز الضحية دون إذن، ومن ثم يُستخدم في اختراق كافة البيانات الخاصة بصاحب الجهاز، وسرقتها أو التّحكم بها أو إتلافها.

6. برمجيات الفدية Ransomware

هي برمجيات تُعدّ الأشهر والأكثر استخدامًا؛ لأنها تستهدف المعلومات السريّة والحساسة، وتدفع هذه الهجمات الضحية لحذف كافة المعلومات على جهازه في حالة عدم دفع الفدية في الوقت المحدّد.

7. هجمات التّصتّ Eavesdropping Attacks

نوع من الهجمات التي تعتمد على التّطفّل، ومن ثم سرقة المعلومات ونقلها عبر شبكة عن طريق جهاز الحاسوب أو جهاز ذكي.

8. هجمات البرمجيات الضارة Malware Attacks

البرمجيات الضارة تم تصميمها خصيصًا لإحداث ضرر أو تلف في جهاز الحاسوب أو الخادم أو العميل أو الشبكة بدون معرفة المستخدم بذلك.

9. حصان طروادة Trojan Horses

نوع من البرمجيات الضارة التي يتم إخفاؤها كمرفقات في رسالة بريد إلكتروني أو ملف مجاني التنزيل، وبمجرد التنزيل تبدأ الأكواد الضارة في العمل ومهاجمة البيانات، والتجسس على المعلومات والأنشطة التي يقوم بها المستخدمون.

10. التنمر عبر الإنترنت Cyber Bulling

هو استخدام التقنيات الرقمية في التنمر، وغالبًا ما يحدث من خلال منصات التواصل الاجتماعي أو منصات المراسلة والألعاب.

11. الاحتيال عبر الإنترنت Online Fraud

من أكثر أساليب الجرائم انتشارًا في الوقت الحالي، وغالبًا ما يستهدف الحصول على البيانات البنكية من أجل سرقة الأرصدة أو التسوق الإلكتروني ببطاقات الآخرين.

12. سرقة البيانات Data Theft

عملية سرقة معلومات رقمية مخزنة؛ سواءً على الأجهزة الذكية أو الخوادم أو السحابة، والتي غالبًا ما تكون معلومات سرية أو فيها انتهاك للخصوصية.



2. 24 مُجَسِّمًا خَاصًّا بِالْأَرْقَام لِبَدْءِ اللَّعِبِ.. كُلُّ مُجَسِّمٍ بِرَقْمٍ وَاحِدٍ فَقَط (مِنْ 24-1).

3. 24 بِطَاقَةً خَاصَّةً بِالمَحَطَّات لِشَرْحِ المِصْطَلَحَاتِ السَّيْبِرَانِيَّةِ الوَارِدَةِ بِهَا، وَتَوْضِيحِ سَبَبِ إِيجَابِيَّةِ المَحَطَّةِ أَوْ خُطُورَتِهَا لِلطَّلَبَةِ.

4. 10 رَمُوزٍ بِلاَسْتِيكِيَّةٍ مُتَوَسِّطَةِ الحَجْمِ تُوزَعُ عَلَى الطَّلَبَةِ فِي بَدَايَةِ اللُّعْبَةِ (مُقَسَّمةً لِمَجْمُوعَتَيْنِ، كُلُّ مَجْمُوعَةٍ لَهَا ٥ أَشْكَالٍ مُخْتَلِفَةٍ بِلَوْنٍ وَاحِدٍ، بِحَيْثُ يَخْتَارُ كُلُّ طَالِبٍ رَمْزًا خَاصًّا يَتَحَرَّكُ بِهِ).



5. 60 بِطَاقَةً خُضراءَ كَبِيرَةً، عِبَارَةٌ عَنْ جَوَائِزٍ مُتَنَوِّعَةٍ، كَالتَّالِي:

- 5 بِطَاقَاتٍ (يُمْكِنُكَ اللَّعِبَ الدَّوْرَ القَادِمَ).
- 5 بِطَاقَاتٍ (تَهَانِينًا.. رَبَحْتَ بِطَاقَةً قَائِدَ الفَرِيقِ).
- 5 بِطَاقَاتٍ (رَبَحْتَ بِطَاقَةً الأَمْنِ السَّيْبِرَانِيَّ).
- 5 بِطَاقَاتٍ (رَبَحْتَ البِطَاقَةَ الذَّهَبِيَّةَ).
- 5 بِطَاقَاتٍ (حَصَلْتَ عَلَى البِطَاقَةِ الفُضِيَّةِ).
- 5 بِطَاقَاتٍ (البِطَاقَةُ البَرُونِزِيَّةُ.. تَهَانِينًا).
- 5 بِطَاقَاتٍ (رَبَحْتَ رَمْزَ المِفْتَاحِ).
- 5 بِطَاقَاتٍ (حَصَلْتَ عَلَى رَمْزِ Wi - Fi).
- 5 بِطَاقَاتٍ (يُمْكِنُكَ / لِفَرِيقِكَ التَّخَلُّصُ مِنْ رَمْزِ العَيْنِ).
- 5 بِطَاقَاتٍ (يُمْكِنُكَ / لِفَرِيقِكَ التَّخَلُّصُ مِنْ رَمْزِ حِصَانِ طُرُودَةِ).
- 5 بِطَاقَاتٍ (حَصَلْتَ عَلَى 2 Coins مِنْ الفَرِيقِ المُنَافِسِ).
- 5 بِطَاقَاتٍ (اخْتَرِ عَقُوبَةً لِلْفَرِيقِ المُنَافِسِ).



6. 60 بطاقة حمراء كبيرة، عبارة عن عُقوبات مختلفة كالتالي:

- 5 بطاقات (لا تلعب الدور القادم).
- 5 بطاقات (غادر الفريق).
- 5 بطاقات (تنازل عن 2 Coins للفريق المنافس).
- 5 بطاقات (خسرت/ خسر فريقك بطاقة القائد).
- 5 بطاقات (حصلت على بطاقة مُتَجَسِّس).
- 5 بطاقات (خسرت/ خسر فريقك البطاقة الذهبية).
- 5 بطاقات (خسرت/ خسر فريقك البطاقة الفضية).
- 5 بطاقات (خسرت/ خسر فريقك البطاقة البرونزية).
- 5 بطاقات (خسرت/ خسر فريقك بطاقة الأمن السيبراني).
- 5 بطاقات (خسرت/ خسر فريقك رمز Wi - Fi).
- 5 بطاقات (حصلت على رمز العين).
- 5 بطاقات (حصلت على رمز حصان طروادة).



7. 40 رمزًا جانبيًا مُلوّنًا كبيرًا يقوم الحَكم بتوزيعها على الطلّبة، كالتالي:

- 10 قِطْع من رَمز المفتاح (الرّمز يساوي 5 Coins).
 - 10 قِطْع من رمز Wi - Fi (الرّمز يساوي 10 Coins).
 - 10 قِطْع من رَمز العين (الرّمز يُفقد صاحبه/ الفريق 5 Coins).
 - 10 قِطْع من رَمز حصان طروادة (الرّمز يُفقد صاحبه/ الفريق 10 Coins).
8. 200 قطعة Coins خاصّة بالجوائز والعقاب، واحتساب النّتيجة النّهائيّة لكلّ فريق.



آلية اللعب

1. اللعبة تعتمد على الأداء الجماعي؛ بحيث يتم تقسيم الطلبة إلى فريقين، يمكن أن يكون الفريق طالباً أو طالبين، على أن يقوم طالب إضافي بدور الحكم لتوزيع الجوائز والعقوبات على أفراد الفريقين.
2. يحصل كل طالب على رمز صغير خاص به للتحرك فوق اللوحة.
3. يقوم الطالب باختيار رقم عشوائي من المجسمات الخاصة بالأرقام، والسير بحسب العدد الذي يظهر له.
4. إذا ما وقف الطالب على محطة آمنة سيحصل على البطاقة التوضيحية الخاصة بها، وسيقرأ المعلومات الواردة فيها لزملائه للنقاش فيها، ثم يختار بين مجموعة من البطاقات الخضراء، وهي عبارة عن جوائز متنوعة، مثل:

- يمكنك اللعب الدور القادم.
- تهانينا.. أصبحت قائد الفريق.
- ربحت البطاقة الذهبية.
- ربحت 2 Coins من الفريق المنافس.
- ربحت رمز المفتاح.



5. إذا ما وقف الطالب على محطة حمراء خطرة سيحصل على البطاقة التوضيحية الخاصة بالمحطات، وسيقرأ المعلومات الواردة فيها لزملائه للنقاش فيها، ثم سيختار بين مجموعة أخرى من البطاقات الحمراء، وهي عبارة عن عقوبات مختلفة مثل:

- لا تلعب الدور القادم.
- غادر الفريق.
- تنازل عن 2 Coins للفريق المنافس.
- حصلت على رمز العين.
- حصلت على بطاقة متجسس.
- خسر فريقك البطاقة الذهبية.

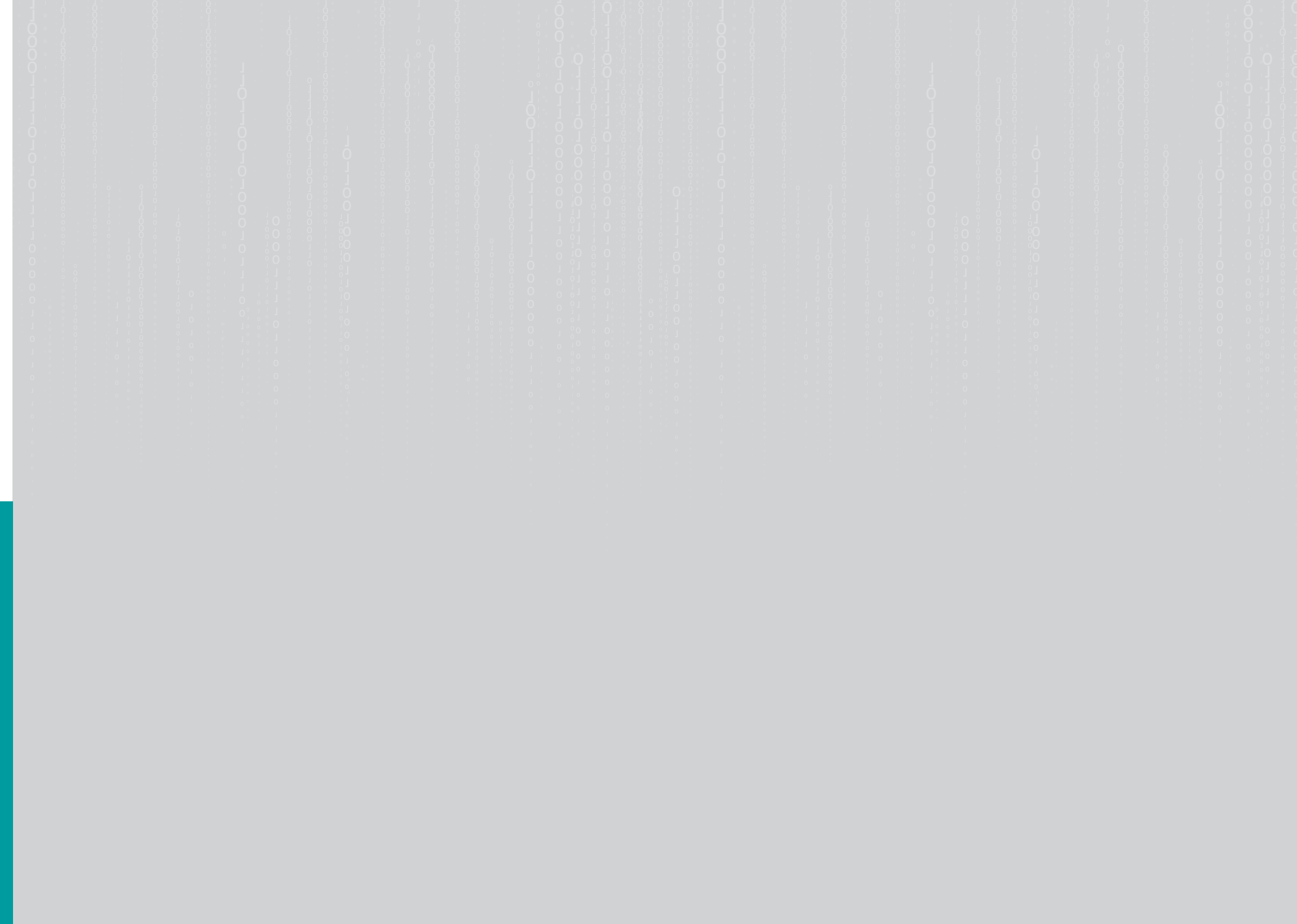


6. تتوالى الأدوار بين الطلّبة، وفي النهاية يتم احتساب عدد النقاط مع كلّ فريق كالتالي:

- رمز المفتاح (الرّمز يساوي 5 Coins).
- رمز Wi - Fi (الرّمز يساوي 10 Coins).
- رمز العين (الرّمز يُفقد صاحبه / الفريق 5 Coins).
- رمز حصان طروادة (الرّمز يُفقد صاحبه / الفريق 10 Coins).
- بطاقة قائد الفريق (نقاطه مضاعفة فإذا كان القائد يملك 5 Coins على سبيل المثال يتم احتساب نقاطه بـ 10 Coins).
- البطاقة الذهبية (البطاقة الذهبية تساوي 15 Coins).
- بطاقة مُتجسّس (البطاقة تُفقد صاحبها/الفريق 10 Coins).

7. الفريق الفائز هو الحاصل على أكبر عدد من النقاط.







اللّعبة الثانية: Cyber Quiz

اللُّعْبَةُ تأخذ الأطفال في جَوْلَةٍ تَنَافُسِيَّةٍ شَيِّقَةٍ من خلال تَوْجِيهِ الأَسْئَلَةِ والإِجَابَةِ عنها في مَوَاضِعَاتٍ سَيِّبَرَانِيَّةٍ مُبَسَّطَةٍ وَسَلِيسَةٍ خلال تَوْقِيتٍ زَمَنِيٍّ مُحَدَّدٍ، كُلُّ هَذَا فِي قَالِبٍ تَنَافُسِيٍّ جَذَابٍ يَضْمَنُ التَّرْفِيهِ والتَّعَلُّمَ بِطَرِيقَةٍ تَنَافُسِيَّةٍ مُبْتَكَرَةٍ.

أهداف اللُّعْبَةِ

1. تعليم الطَّلَبَةِ مُصْطَلَحَاتٍ سَيِّبَرَانِيَّةٍ جَدِيدَةٍ وَمُبَسَّطَةٍ.
2. التَّعَرُّفُ عَلَى مَزَايَا أَوْ خُطُورَةِ المِصْطَلَحَاتِ السَيِّبَرَانِيَّةِ الجَدِيدَةِ.
3. تَنْمِيَةِ المَهَارَاتِ اللُّغَوِيَّةِ والمَعْرِفِيَّةِ فِي المَجَالِ السَيِّبَرَانِيَّ لِلطَّلَبَةِ.
4. تَرْسِيخُ الأَسَاسِ المَعْرِفِيَّةِ فِي الأَمْنِ السَيِّبَرَانِيَّ لَدَى الطَّلَبَةِ مِنْ خِلَالِ عُنْصَرِي التَّرْفِيهِ والتَّنَافُسِ.
5. كِتَابَةِ المِصْطَلَحَاتِ بالعَرَبِيَّةِ والإنْجِلِيزِيَّةِ سَيِّسَاعِدَ بِشَكْلٍ مُبَاشِرٍ فِي تَحْسِينِ المَهَارَاتِ اللُّغَوِيَّةِ، والقُدْرَةِ عَلَى القِرَاءَةِ.
6. إعْطَاءُ الأَطْفَالِ جُرْعَةً مِنَ الحِمَاسِ والتَّسْلِيَةِ، والشُّعُورِ بِالإِنْجَازِ عَنْ طَرِيقِ التَّنَافُسِ بَيْنَ الطَّلَبَةِ عَلَى اكْتِسَابِ أَكْبَرِ قَدْرٍ مِنَ النِّقَاطِ بِالإِجَابَةِ الصَّحِيحَةِ عَنْ الأَسْئَلَةِ السَيِّبَرَانِيَّةِ.

السَّنُ الْمُنَاسِبَةُ لِلُّعْبَةِ

7+ سنوات



مُكوّنات اللعبة



1. 25 مُجَسِّمًا/ رمزًا بلاستيكيًا مُتوسِّط الحجم خاصّ بالأرقام من 1-25، كلّ مجسّم برقم مُختلف.
2. 100 قطعة Coins (مُتوسِّطة الحجم) تُوزَّع على الطلبة عند الإجابة الصحيحة عن الأسئلة.
3. 25 بطاقة خاصّة بالموضوعات السيبرانيّة، كلّ بطاقة تتناول موضوعًا سيبرانيًا مُعيَّنًا، وتُحوي البطاقات أيضًا أهمّ المَعْلُومَات المُختصرة عن الموضوع أو المصطلح بصورة مُبسَّطة وسليسة (كلّ بطاقة مُرقّمة من 1 - 25 مع عنوان البطاقة).
4. 100 بطاقة سؤال؛ لكلّ مَوْضوع أربع بطاقات عبارة عن أسئلة خاصّة بالمصطلح السيبرانيّ الذي تستعرضه البطاقة، ويجب أن يُجيب عنها الطّالِب حتى يحصل على نقاط (بطاقة واحدة لكلّ سؤال).
5. فلاير يضمّ نموذج إجابات الأسئلة الخاصّة بالموضوعات السيبرانيّة.
6. مُوقّت زمنيّ لاحتساب وقت الإجابة عن كلّ سؤال (ساعة رملية صغيرة).
7. دليل اللعبة.

آلية اللعب

1. اللّعبة تعتمد على الأداء الفردي (بحدّ أقصى 5 طلبة)، فيتنافس كلّ طالب مع باقي زملائه على القوْز والحصول على أكبر عددٍ من الـ Coins (النّقاط).
2. يقوم أحد الطّلبة بدوْر الحَكَم لتوزيع الأسئلة على باقي الطّلبة وتقييم الإجابات.
3. في البداية، يُفرد لوح اللعب أمام الطّلبة، وتوضّع البطاقات والسّاعة الرّمليّة في أماكنها على اللّوح.
4. يقوم كلّ طالب باختيار رَقْم عشوائيّ من مُجسّمات الأرقام، وصاحب الرّقْم الأكبر هو الذي يبدأ اللّعب.
5. يَسحب الطّالب بطاقة الموضوع السيبرانيّ بحسب الرّقْم، ويقرأ المَقْلُومَات الواردة فيها بصوتٍ مرتفعٍ، ويتناقش فيها مع زملائه والحَكَم.

6. بعد ذلك يقوم الحَكَم بتوجيه أحد أسئلة هذه البطاقة للطّالب، وبدء التّوقيت الزمنيّ للإجابة عنه.
7. إذا أجاب الطّالب عن السّؤال قبل انتهاء التّوقيت الزّمنيّ إجابة صحيحة يَحْضُل على قطعةٍ واحدةٍ من الـ Coins (القطعة الواحدة تُساوي نقطةً واحدةً).
8. إذا لم يُجب الطّالب عن السّؤال خلال الوقت المُحدّد له بالتوقيت الزمنيّ فلا يحصل على شيءٍ.
9. إذا أجاب الطّالب عن السّؤال إجابةً خاطئةً فلا يحصل على شيءٍ.
10. تتوالى الأدوار بين الطّلبة، وخلال اللعبة يحرص كلّ طالب على تجميع أكبر قدر مُمكن من الـ Coins (النّقاط).
11. الطّالب الفائز هو الحاصل على أكبر قدر مُمكن من الـ Coins (النّقاط).



موضوعات البطاقات السَّيرانيَّة وأسئلتها

الموضوع الأول: سَلَامَة البيانات Data integrity

بياناتك ومعلّوماتك الشَّخصيَّة أمرٌ مهمٌ يجب الحِفاظ عليه وحمايته من الهجمات التَّخريبية أو السرقة.

البطاقات الأربعة للموضوع

1. صورة لمحفظة وهويَّة ويد مُمتدَّة لأخذها.. صحيح أم خطأ؟
2. مُحادثاتنا عبر واتس آب نُطْلِع عليها الآخرين.. صحيح أم خطأ؟
3. صُورنا الشَّخصيَّة والعائليَّة لا نُشاركها مع الغرباء.. صحيح أم خطأ؟
4. تخصيص منشوراتنا على "فيسبوك" للأصدقاء فقط.. صحيح أم خطأ؟



الموضوع الثَّاني: جدار الحماية Firewall

هو أداة مُخصَّصة أو برنامج على جهاز الحاسوب تمنع انتشار البرمجيات الضَّارة عَبْر مُرَاقَبَة العمليَّات التي تَمُرُّ بشبْكة الإنترنت، ورَفُض أو السَّماح للبيانات بالمُرُور طبقاً لقواعد مُعيَّنة.

البطاقات الأربعة للموضوع

1. جُدْران الحماية قد تكون برامج أو أدوات.. صحيح أم خطأ؟
2. جدار الحماية أداة أمان.. صحيح أم خطأ؟
3. لا يرتبط جدار الحماية بشبكة الإنترنت.. صحيح أم خطأ؟
4. يَمنع جدار الحماية انتشار البرمجيات الضَّارة.. صحيح أم خطأ؟



الموضوع الرابع: أمن التطبيقات Application security

توفّر تطبيقات المراسلة طريقة سهلة للتواصل مع الأصدقاء، لكنها قد تُشكّل تهديدًا للخصوصية إذا ما تمّ خرق البيانات من خلالها، لذا عند استخدامها من الضروريّ تطبيق قواعد الأمان.

البطاقات الأربعة للموضوع

1. لا تُشكّل تطبيقات المراسلة تهديدًا لبيانات الأفراد.. صحيح أم خطأ؟
2. واتس آب (WhatsApp) أحد أشهر تطبيقات المراسلة والتّواصل مع الأصدقاء.. صحيح أم خطأ؟
3. تشفير البيانات في تطبيقات المراسلة لا يحمي الخصوصية.. صحيح أم خطأ؟
4. اتباع قواعد الأمان في تطبيقات المراسلة يمنع خرق البيانات.. صحيح أم خطأ؟



الموضوع الثالث: أمن المعلومات Information security

عملية تصميم واستخدام أدوات من أجل حماية المعلومات المهمة من التّلف أو الضّياع أو التّعديل أو التّعطّل، خاصّة في حالة النّقل أو التّخزين.

البطاقات الأربعة للموضوع

1. المعلومات عبارة عن بيانات مُجهّزة في الحاسوب بشكلٍ مُنظّم.. صحيح أم خطأ؟
2. أمن المعلومات هو استخدام أدوات لحماية البيانات المهمة.. صحيح أم خطأ؟
3. أمن المعلومات هو حماية البيانات المُخزّنة في أجهزة الحاسوب.. صحيح أم خطأ؟
4. حماية البيانات من التّلف أحد أهداف أمن المعلومات.. صحيح أم خطأ؟



الموضوع الخامس: مُخترِقو الأجهزة والبيانات Hackers

مُخترِقو الأجهزة والبيانات هم مُجرِّمون رَقْمِيَّون ذوو إمكانيَّات برمجية وتقنية عالية في التَّعامل مع البرامج والشبكات وبنية الحاسب، يَستغلُّون خبراتهم التقنية لأهدافٍ مختلفةٍ قد تكون السَّرقة، أو التَّشهير، أو التَّخريب، أو حتى مُجرَّد العبث لإثبات كفاءته العالية.

البطاقات الأربعة للموضوع

1. المُخترِق هو شَخْص يحصل على المَعلُومَات بطريقة قانونية.. صحيح أم خطأ؟
2. المُخترِق يَتمتع بِقُدرات برمجية وتقنية عالية.. صحيح أم خطأ؟
3. يَستخدم المُخترِق في عَمَله التَّفَرُّات الأُمْنِيَّة بِشكلٍ رَئيس.. صحيح أم خطأ؟
4. سرقة البيانات ليست من أهداف الهاكرز.. صحيح أم خطأ؟



الموضوع السادس: الهجوم الإلكتروني Cyber-Attack

هو هُجوم من قَرْد أو مُنظَّمة للتَّحكُّم بالبيانات أو تَعديلها أو تَدميرها بِاستخدام الفضاء الإلكتروني، وغالبًا ما يَستهدف المُؤسَّسات من أَجل تَدميرها أو الإضرار بِها وبسلامة البيانات والمَعلُومَات التي تحتوي عليها.

البطاقات الأربعة للموضوع

1. الهُجوم الإلكتروني يجب أن يَتمَّ بِواسطة شبكات الإنترنت.. صحيح أم خطأ؟
2. المُجرِّم الإلكتروني قد يكون شَخْصًا أو مُنظَّمة.. صحيح أم خطأ؟
3. تخريب الأجهزة الإلكترونية ليس نوعًا من الهُجوم الإلكتروني.. صحيح أم خطأ؟
4. تسجيل الخُروج من الحَساب على حاسوب في صالة عامَّة .. صحيح أم خطأ؟



الموضوع الثامن: الجريمة الإلكترونية Cybercrime

هي شكل مُتطوّر من الجريمة، وتُحدّث على نطاقٍ عالميٍّ، وتُستهدف الحواسيب أو الشبكات أو البنى التحتية.

البطاقات الأربعة للموضوع

1. صورة لأحدهم يُرسل رسالةً غامضةً أو تهديدًا.. طفل يَظهر وهو ينادي والده لرؤية الرسالة التي وصلتته.. صحيح أم خطأ؟
2. تُرتكب الجرائم الإلكترونية من قِبَل مُجرمي الإنترنت.. صحيح أم خطأ؟
3. لا تُؤثّر الجرائم الإلكترونية سلبيًا على الضحايا.. صحيح أم خطأ؟
4. كلمة سِرّ مُعقّدة طويلة فيها رموز وأحرف كبيرة وصغيرة وأرقام.. صحيح أم خطأ؟



الموضوع السابع: البرمجيات الضارة Malware

البرمجيات الضارة تمّ تصميمها خصيصًا لإحداث ضرر أو تلف في جهاز الحاسوب أو الخادم أو العميل أو الشبكة بدون معرفة المُستخدم بذلك، وتنتقل بشكل رئيس عبر البريد الإلكتروني.

البطاقات الأربعة للموضوع

1. تُصيب البرمجيات الضارة الحواسيب.. صحيح أم خطأ؟
2. البريد الإلكتروني أحد أكثر الطرق المعروفة لنشر البرمجيات الضارة.. صحيح أم خطأ؟
3. البرمجيات الضارة لا تُستهدف سرقة أو إتلاف البيانات.. صحيح أم خطأ؟
4. برامج الحماية تمنع انتشار البرمجيات الضارة داخل الحاسوب.. صحيح أم خطأ؟



الموضوع العاشر: التَّثْمُر عبر الإنترنت Cyberbullying

هو استخدام التقنيات الرقمية في التَّثْمُر، وغالبًا ما يحدث من خلال منصات التواصل الاجتماعي أو منصات المراسلة والألعاب، ويترك التَّثْمُر عبر الإنترنت بَصْمَةً رقمية يمكن تتبعها وكشف صاحبها.

البطاقات الأربعة للموضوع

1. طفل ينفلق على نفسه ورفاقه يتتَمَرُون عليه ويوجَّهون له الكلام المسيء.. صحيح أم خطأ؟
2. تعليقات مُسيئة عبر وسائل التواصل الاجتماعي.. صحيح أم خطأ؟
3. قد يحدث التَّثْمُر عبر الإنترنت عبر وسائل التواصل الاجتماعي.. صحيح أم خطأ؟
4. لا يترك التَّثْمُر عبر الإنترنت بَصْمَةً رقمية.. صحيح أم خطأ؟



الموضوع التاسع: برنامج حصان طروادة Trojan Horses

يُسمَّى أيضًا "لص الألعاب"، وهو من البرمجيات الضارة التي يتم إخفاؤها كمرفقات في رسالة بريد إلكتروني أو ملف مجاني التنزيل، وبمجرد التنزيل تبدأ الأكواد الضارة في العمل ومهاجمة البيانات، والتجسس على المعلومات والأنشطة التي يقوم بها المستخدمون.

البطاقات الأربعة للموضوع

1. يتسبب برنامج حصان طروادة في مهاجمة البيانات.. صحيح أم خطأ؟
2. لا يحمل برنامج حصان طروادة أي أكواد ضارة.. صحيح أم خطأ؟
3. يُطلق على برنامج حصان طروادة «لص الألعاب».. صحيح أم خطأ؟
4. يتجسس برنامج حصان طروادة على بيانات الأفراد.. صحيح أم خطأ؟



الموضوع الثاني عشر: الممارسات التكنولوجية الآمنة Safe technology practices

أوجدت التكنولوجيا ومواقع التواصل الاجتماعي نوعًا جديدًا من الممارسات الفردية، والتي تتنوع بين الإيجابية والسلبية، وحتى يتمكن الأفراد من الاستفادة المثلى من الطفرة التكنولوجية المستمرة يجب عليهم التفرقة بين هذه الممارسات، وتجنب السلبية منها.

البطاقات الأربعة للموضوع

1. الجلوس في وضعية غير مستوية أمام الحاسوب .. صحيح أم خطأ؟
2. أخذ موافقة صاحب صورة معينة قبل نشرها .. صحيح أم خطأ؟
3. الألعاب الإلكترونية التي توحى بالعنف، لا تعد جيدة للأطفال.. صحيح أم خطأ؟
4. صورة لطفل يجلس أمام حاسوبه لمدة طويلة تظهر على الساعة في الصورة، وأمامه الأطعمة والعصير .. صحيح أم خطأ؟



الموضوع الحادي عشر: سرقة البيانات Data Theft

عملية سرقة معلومات رقمية مخزنة؛ سواء على الأجهزة الذكية أو الخوادم أو السحابة، والتي غالبًا ما تكون معلومات سرية أو فيها انتهاك للخصوصية، ويتم ذلك عبر رسائل الجوال أو البريد الإلكتروني المضللة.

البطاقات الأربعة للموضوع

1. الضبط على إعلان مُزيّف للفوز بجهاز لوحي .. صحيح أم خطأ؟
2. فتح رسائل مجهولة المصدر يؤدي إلى خرق البيانات الشخصية.. صحيح أم خطأ؟
3. منح بياناتنا المصرفية لجهات غير موثوقة .. صحيح أم خطأ؟
4. سرقة البيانات لا تؤدي إلى حدوث خسائر مادية .. صحيح أم خطأ؟



الموضوع الثالث عشر: الاحتيال عبر الإنترنت Online Fraud

من أكثر أساليب الجرائم انتشارًا في الوقت الحالي، وغالبًا ما يستهدف الحصول على البيانات البنكية من أجل سرقة الأرصدة أو التسوّق الإلكتروني بطاقات الآخرين.

البطاقات الأربعة للموضوع

1. يستهدف الاحتيال عبر الإنترنت خداع الضحايا للحصول على بيانات مالية.. صحيح أم خطأ؟
2. مسح رسالة مجهولة على الهاتف، تقول «مبروك! ربحت جائزة كبرى!».. صحيح أم خطأ؟
3. مشاركة بيانات الهاتف والمعلومات الشخصية عبر مواقع التواصل الاجتماعي.. صحيح أم خطأ؟
4. غالبًا ما يستهدف الاحتيال عبر الإنترنت الحصول على البيانات البنكية.. صحيح أم خطأ؟



الموضوع الرابع عشر: ديدان الحاسوب Computer Worms

برمجيات ضارة تتكاثر وتنتشر ضمن الأجهزة، يمكن للديدان إبطاء أداء الحاسوب وتخريب العمليات وسرقة البيانات.

البطاقات الأربعة للموضوع

1. يُبطئ أداء الحاسوب من علامات وجود الديدان.. صحيح أم خطأ؟
2. فتح رسالة بريد مجهولة المصدر فيها مُرفق.. صحيح أم خطأ؟
3. ديدان الحاسوب تتكاثر وتنتشر.. صحيح أم خطأ؟
4. تستخدم الديدان ذاكرة الجهاز فيتبطل الجهاز.. صحيح أم خطأ؟



الموضوع الخامس عشر: الحوسبة السحابية Cloud Computing

مكان آمن عبر الإنترنت تحتفظ به بنسخة من البيانات، يمكننا العودة إليها في أي وقت ومشاركتها مع الآخرين بإرسال رابط (URL) فقط، ويمكن استخدام المزامنة والوصول للبيانات من خلال أجهزة متعددة.

البطاقات الأربعة للموضوع

1. يمكن استرجاع البيانات من السحابة في أي وقت.. صحيح أم خطأ؟
2. لا يمكن مشاركة بيانات السحابة مع الآخرين.. صحيح أم خطأ؟
3. النسخ الاحتياطي لبياناتك على السحابة يحمي بياناتك.. صحيح أم خطأ؟
4. لا يمكن استخدام خدمات السحابة الإلكترونية بدون توفر الإنترنت.. صحيح أم خطأ؟



الموضوع السادس عشر: الذباب الإلكتروني Electronic Flies

يسمى بالجيش الإلكتروني، وهو مجموعة حسابات وهمية تنشط عبر وسائل التواصل الاجتماعي، لا يتحكم بها أشخاص حقيقيون تهدف إلى نشر معلومات خاطئة للتأثير في الرأي العام، ترتبط بالتصيد الاحتيالي وسرقة أموال البنوك والمعلومات.

البطاقات الأربعة للموضوع

1. الذباب الإلكتروني حسابات وهمية تنشط عبر وسائل التواصل الاجتماعي.. صحيح أم خطأ؟
2. الذباب الإلكتروني يهدف لنشر معلومات خاطئة.. صحيح أم خطأ؟
3. خرق بيانات البنوك من الأهداف الرئيسة لهجمات الذباب الإلكتروني.. صحيح أم خطأ؟
4. يطلق على الذباب الإلكتروني "الجيش الإلكتروني".. صحيح أم خطأ؟



الموضوع السابع عشر: استراق النظر Shoulder Surfing

خدعة هندسية اجتماعية يقوم من خلالها شخص ما بالتلصص على حاسوبك وسرقة معلومات سرية، القرص الرئيسي من هذه الحيلة هو سرقة المعلومات المالية، مثل: تفاصيل بطاقة الائتمان أو كلمات مرور الحساب.

البطاقات الأربعة للموضوع

1. في الأماكن العامة انتبه جيدًا لوقوف أحدهم خلفي أثناء إدخال كلمة المرور.. صحيح أم خطأ؟
2. أستخدم شاشة الخصوصية على أجهزتي؛ حتى لا يرى الواقف بجانبني ما أفعله في أجهزتي .. صحيح أم خطأ؟
3. استراق النظر يُشبه التنصت والاستماع لخصوصيات الآخرين.. صحيح أم خطأ؟
4. من خلال استراق النظر يمكن سرقة البيانات.. صحيح أم خطأ؟



الموضوع الثامن عشر: حماية هاتفي الذكي Smartphone Security

لا بُد من حماية هاتفنا الذكي والتحديث الدائم لنظامه، والحرص عليه من أي عملية اختراق قد تُصيبه بالسُخونة أو سُرعة نفاذ الشَّحن؛ حيث يمكن سرقة بياناتنا ومعلوماتنا الشخصية عبر الشبكات العامة أو التطبيقات غير المرخصة.

البطاقات الأربعة للموضوع

1. سُخونة جهازي، وسُرعة نفاذ الشَّحن قد تكون علامة على خرق الجهاز.. صحيح أم خطأ؟
2. تجنّب استخدام الشبكات العامة قدر الإمكان.. صحيح أم خطأ؟
3. تثبيت التطبيقات من خارج المتجر الرسمي يحمي جهازي من الخرق.. صحيح أم خطأ؟
4. التحديث الدائم لنظام الهاتف يحميه من التهديدات المُحتملة .. صحيح أم خطأ؟



الموضوع التاسع عشر: كلمات المرور Password

كلمات المرور Password هي أداة حماية تُستخدم لحماية البرامج والتطبيقات؛ بحيث لا يتمكن من دخول التطبيقات أو الاطلاع على البيانات إلا المُستخدم، ويحمي بذلك بياناته من القَبْث والسرقة.

البطاقات الأربعة للموضوع

1. يتم كتابة كلمة مرور واحدة لكل التطبيقات.. صحيح أم خطأ؟
2. يجب أن تحتوي كلمات المرور على أرقام وأحرف ورموز.. صحيح أم خطأ؟
3. يجوز مشاركة كلمات المرور مع الأصدقاء.. صحيح أم خطأ؟
4. 123456789 مثال عن كلمة مرور قوية.. صحيح أم خطأ؟



الموضوع العشرون: الألعاب الإلكترونية E-Games

الألعاب الإلكترونية مُفيدة ومُفيدة للأطفال، لكن الألعاب مع الأصدقاء أكثر فائدة ومُتعة.

البطاقات الأربعة للموضوع

1. قضاء وقتٍ طويلٍ واستخدام الألعاب الإلكترونية ضرره أكبر من نفعه.. صحيح أم خطأ؟
2. بعض الشعارات التي تظهر في الألعاب الإلكترونية لا تناسب ديننا وأخلاقنا -مثل علم قوس قزح-.. صحيح أم خطأ؟
3. لعب الألعاب الإلكترونية لساعاتٍ طويلة.. صحيح أم خطأ؟
4. الألعاب الإلكترونية التي لعب بها يجب أن تكون مناسبة لعمري وبعيدة عن العنف.. صحيح أم خطأ؟



الموضوع الثاني والعشرون: حماية البريد الإلكتروني Email Security

يستخدم مُجرمو الإنترنت البريد الإلكتروني لتنفيذ العديد من جرائمهم؛ من خلال إرسال مُرفقات تحوي برمجيات ضارة، أو من خلال محاولة اختراق البريد الإلكتروني للمستخدم والاطلاع على بياناته الشخصية.

البطاقات الأربعة للموضوع

1. لا بُدَّ من تغيير كلمة المرور المُختصة بالبريد الإلكتروني بشكلٍ دوريٍّ.. صحيح أم خطأ؟
2. لا يجوز فتح المُرفقات الواردة من مجهولين.. صحيح أم خطأ؟
3. يُفضَّل اختيار كلمة مرور للبريد الإلكتروني سهلة التّخمين.. صحيح أم خطأ؟
4. تحديث برامج الحماية من البرمجيات الضّارة يحمي البريد الإلكتروني من الخرق.. صحيح أم خطأ؟



الموضوع الحادي والعشرون: التّصيد الاحتياليّ Phishing

التّصيد الاحتياليّ أسلوبٌ للاحتيال يُستخدمه مُجرمو الإنترنت لسرقة البيانات الشخصية للمستخدمين، من خلال خداعهم، بهدف الإضرار بهم.

البطاقات الأربعة للموضوع

1. تجاهل الرسائل الواردة من مجهولين يحمي من هجمات التّصيد الاحتياليّ.. صحيح أم خطأ؟
2. استخدام كلمات مرور قويّة يحمي من هجمات التّصيد الاحتياليّ.. صحيح أم خطأ؟
3. فتح المُرفقات الواردة من مجهولين عن طريق البريد الإلكتروني يحمي من هجمات التّصيد الاحتياليّ.. صحيح أم خطأ؟
4. عدم مُشاركة البيانات الشخصية مع الآخرين يحمي من هجمات التّصيد الاحتياليّ.. صحيح أم خطأ؟



الموضوع الرابع والعشرون: قواعد التصفح الآمن للإنترنت Rules for Safe Internet Browsing

اتباع قواعد التصفح الآمن للإنترنت يحمي المستخدم من التعرض للهجمات الإلكترونية، ومن سرقة بياناته الشخصية ومن ابتزازه إلكترونياً.

البطاقات الأربعة للموضوع

1. لا يجوز تحميل التطبيقات من مواقع غير موثوقة.. صحيح أم خطأ؟
2. الإعلانات الإلكترونية لا تُشكل مصدرًا من مصادر التهديد الإلكتروني.. صحيح أم خطأ؟
3. يُفضل الاحتفاظ بكلمة المرور واسم المستخدم في مكان واحد.. صحيح أم خطأ؟
4. لا يجوز قبول طلبات الصداقة من أشخاص مجهولين.. صحيح أم خطأ؟



الموضوع الثالث والعشرون: التعلم الإلكتروني E-learnin

في ظلّ جائحة كورونا وما بعدها أخذ التعلم الإلكتروني والدُّروس الافتراضية بالانتشار أكثر فأكثر، وذلك عبر منصات وتطبيقات مختلفة؛ ما يعني أنّ التكنولوجيا بيد الأطفال أكثر، لا بُدّ من زيادة وعي الأطفال وحماية الشبكات المنزلية أكثر.

البطاقات الأربعة للموضوع

1. يمكن تعلم الكثير من الأشياء عن بُعد عبر الإنترنت.. صحيح أم خطأ؟
2. هناك منصات وتطبيقات محدودة يمكن استخدامها للتعلم الإلكتروني.. صحيح أم خطأ؟
3. حماية الشبكات المنزلية حتى لا تُتخرق عند استخدام الأطفال للأجهزة الإلكترونية.. صحيح أم خطأ؟
4. قد يكون التعلم الإلكتروني مفيداً للأطفال ولكن بضوابط معينة.. .. صحيح أم خطأ؟



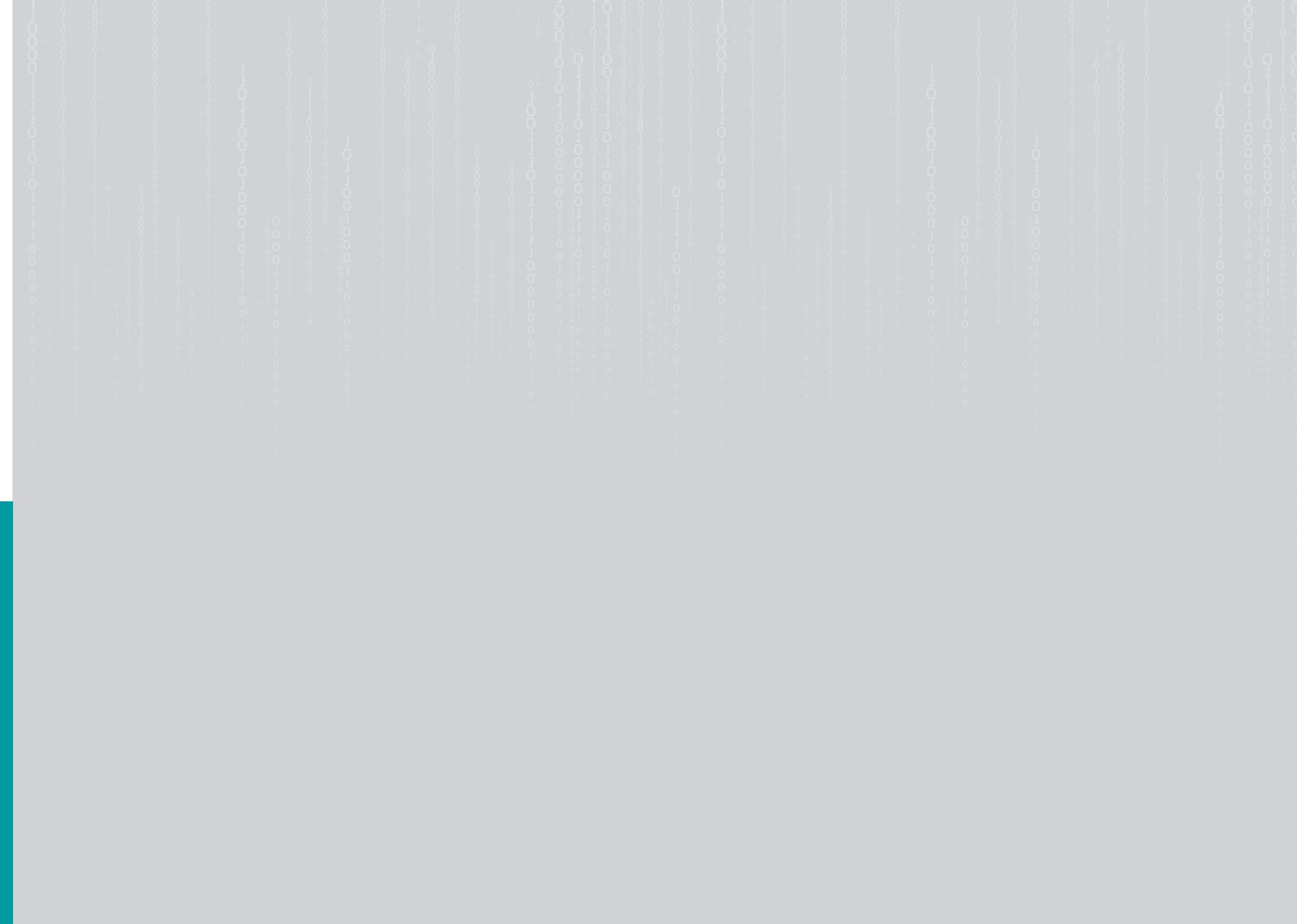


الموضوع الخامس والعشرون: الابتزاز الإلكتروني Electronic Blackmail

وهي المطالبة بالمال أو المعلومات من الأشخاص والشركات عن طريق التهديد بنشر أمور خاصة وبيانات سرية على وسائل التواصل الاجتماعي. ويُعد الأطفال من أكثر الفئات المعرضة للابتزاز الإلكتروني.

البطاقات الأربعة للموضوع

1. الابتزاز الإلكتروني هو المطالبة بالمال من خلال التهديد بنشر أمور خاصة.. صحيح أم خطأ؟
2. توجد طرق مختلفة يتم بها تنفيذ الابتزاز الإلكتروني.. صحيح أم خطأ؟
3. الأطفال من أكثر الفئات المعرضة للابتزاز الإلكتروني .. صحيح أم خطأ؟
4. قد تكون الدوافع وراء الابتزاز الإلكتروني مادية.. صحيح أم خطأ؟





اللّعبة الثالثة: Cyberno



الفكرة الأساسية من لعبة "Cyberno" هي توعية طلبة المرحلة الثانوية بمصطلحات ومفاهيم الأمن السيبراني، وكذلك مخاطر وتهديدات الأمن السيبراني بطريقة أكثر قدرة على تحفيز التفكير والربط بين المعلومات السيبرانية، تسهم في اكتساب المعلومات وفق آلية تنافسية مبتكرة، واللعبة تشاركية جماعية ما يضيفي جوا تنافسيا حماسيا.

أهداف اللعبة

1. إيصال المعلومات المهمة للطلبة حول الأمن السيبراني وأبرز مؤوضعاته، وتحديدًا الجرائم السيبرانية.
2. توليد شعور بالفخر لدى الطلبة نتيجة اجتياز كافة المصاعب التي سيتعرض لها أثناء اللعب.
3. إكساب الطلبة مهارة التفكير السريع والتخطيط من خلال دأبهم على العقل لتخطي العقبات التي يتعرضون لها.
4. إذكاء روح التنافس بين الطلبة من خلال تحفيز كل طالب على الفوز.
5. فهم المعاني الخاصة بأبرز المصطلحات الإلكترونية/ السيبرانية، ورفع الوعي بالمخاطر والتهديدات.

السن المناسبة للعبة

17+ سنة

مُكوّنات اللعبة

عدد 116 بطاقة، مُقسّمة إلى أربعة ألوان؛ الأزرق، الأصفر، الأحمر، والأخضر، تلك البطاقات تشمل:

أولاً: عدد 4 بطاقات- 1 بطاقة من كُل لون، وتشمل موضوعات سيبرانية رئيسة كالتالي:

1. الاحتيال عبر الإنترنت Online Fraud: من أكثر أساليب الجرائم انتشاراً في الوقت الحالي، وغالباً ما يستهدف الحصول على البيانات البنكية من أجل سرقة الأرصدة عبر بطاقات الآخرين.
2. الهجمات الإلكترونية Cyber-Attacks: هجمات هدفها التّحكم أو إفساد البيانات أو تعطيل وتدمير الأجهزة وأنظمة التشغيل، وغالباً ما تستهدف المؤسسات للإضرار بها وبسلامة بياناتها.
3. التسلل Intrusion: مصطلح يُستخدم لوصف التقنيات المُستخدمة لجعل البرنامج الضار يدخل لجهاز الضحية بشكل غير واضح، أو إخفاء أيّ تغييرات نفّذها البرنامج الضار على النظام المُصاب.
4. هجوم البريد العشوائي Spam attack: هو استخدام أنظمة المراسلة لإرسال رسالة غير مرغوب فيها، بشكل متكرر، إلى نفس المواقع (المتلقي)، وينتج عنها الاحتيال وتشبّع خادم البريد الإلكتروني وانتشار البرمجيات الضارة وانخفاض سعة التخزين.



ثانيًا: عدد 72 بطاقة تشمل موضوعات سيبرانية متنوعة، منها:

1. أمن الشبكات Network security: ممارسة تأمين شبكة الحاسوب من المتطفلين من خلال تكنولوجيا البرامج والأجهزة المختلفة، وتشمل جدار الحماية، وأمان البريد الإلكتروني.
2. أمن المعلومات Information security: تصميم ونشر أدوات لحماية المعلومات من التلّف أو الضياع أو التعديل أو التعطّل، خاصة في حالة النقل أو التخزين، ويشمل التشفير وإدارة نقاط الضعف.
3. أمن التطبيقات Application security: ويركّز على إبقاء البرامج والأجهزة خالية من أيّ تهديدات، ويتم ذلك عادةً في أثناء مرحلة التصميم، وقبل عملية نشر البرنامج أو الجهاز بوقتٍ طويل.
4. الأمن التشغيلي Operational Security: عملية إدارة المخاطر لجميع عمليات الأمن السيبراني الداخلية، ويشمل هذا العمليات والقرارات الخاصة بمعالجة أصول البيانات وحمايتها.



5. الأمن السحابي Cloud security: يتضمّن حماية أنظمة التخزين السحابية الأساسية في كلّ الأوقات؛ لما عليها من كمّيات هائلة من البيانات، ويتضمّن أيضًا خدمات الأعمال المُخزّنة في مركز البيانات.
6. أمن البنية التحتية Infrastructure security : إجراء أمنيّ يحمي البنية التحتية الحيوية، مثل أنظمة الاتصالات، أو مراكز البيانات والخوادم لحمايتها من العمليات الإرهابية أو الإفساد والتّخريب.
7. الردّ السّيرانيّ Cyber Deterrence: هو كلّ ما يتعلّق بمنع الأعمال الضّارة والهجمات التي قد تحدث في الفضاء السّيرانيّ.
8. الجريمة الإلكترونيّة Cybercrime: هي شكّل مُتطوّر من الجريمة، وتحدث على نطاق عالميّ، وتستهدف الحواسيب أو الشّبكات أو البنى التحتية.
9. هجمات التّصيد الاحتياليّ Phishing Attacks: نوع من الهجمات يهدف إلى سرقة أو إتلاف البيانات الحسّاسة؛ من خلال خداع الأشخاص للحصول على بياناتهم الشّخصيّة والتّحكّم بها.
10. هجمات التّصيد الاحتياليّ المُوجّه Spear Phishing Attacks: عملية احتيال تتمّ من خلال البريد الإلكترونيّ أو الاتّصالات الإلكترونيّة، لسرقة البيانات، وغالبًا ما تعتمد على تثبيت برمجيات ضارة على جهاز الضّحية.



11. هجمات التصيد الاحتيالي الموجه لكبار الشخصيات :Whale Phishing Attacks :
نوع من الهجمات التي تستهدف بشكل خاص المعلومات الحساسة والسرية، خاصة للأثرياء والمشاهير، من أجل الابتزاز أو الحصول على مقابل لتلك البيانات.
12. هجمات التشفير Encryption Attacks : برنامج نصي ضار يقوم بتحميل نفسه تلقائياً، ويثبت نفسه على جهاز الضحية دون إذن، ومن ثم يُستخدم في اختراق كافة البيانات الخاصة بصاحب الجهاز، وسرقتها أو التحكم بها.
13. برمجيات الفدية Ransomware: برمجيات تستهدف المعلومات السرية والحساسة، وتؤدي لإغلاق الأجهزة وأنظمة التشغيل أو تشفير البيانات المهمة، فلا يستطيع صاحبها الوصول إليها إلا بعد دفع الفدية.
14. هجمات التنصت Eavesdropping Attacks: نوع من الهجمات التي تعتمد على التنصت، ومن ثم سرقة المعلومات ونقلها عبر شبكة عن طريق جهاز الحاسوب أو جهاز ذكي.
15. هجمات البرمجيات الضارة Malware Attacks : البرمجيات الضارة تم تصميمها خصيصاً لإحداث ضرر أو تلف في جهاز الحاسوب أو الخادم أو العميل أو الشبكة بدون معرفة المستخدم بذلك.



16. حصان طروادة Trojan Horses: نوع من البرمجيات الضارة التي يتم إخفاؤها كمرفقات في رسالة بريد إلكتروني أو ملف مجاني التنزيل، وبمجرد التنزيل تبدأ الأكواد الضارة في العمل ومهاجمة البيانات.

17. هجمات التنصت الوسيط Man in the middle Attack : نوع من هجمات التنصت، وغالبًا ما تستهدف المحادثات الموجودة بالفعل أو البيانات السريّة التي تم مشاركتها بين طرفين.

18. جدار الحماية Firewall : هو أداة مخصصة أو برنامج على جهاز الحاسوب يقوم بمراقبة العمليات التي تمر بالشبكة، ويرفض أو يسمح فقط بمرور برنامج طبقًا لقواعد معينة.

19. البرمجيات الخبيثة Malware: برمجيات ضارة يتم تصميمها بهدف إحداث ضرر لجهاز الحاسوب المحمول أو جهاز الحاسوب المكتبي أو الجهاز المحمول قد يُبطئ عمله، أو قد يتوقف عن العمل تمامًا.

20. ديدان الحاسوب Computer worms: نوع من البرمجيات الضارة يمكنها نسخ نفسها، وغالبًا ما تنتشر عبر الشبكة عن طريق استغلال الثغرات الأمنية.



21. أدوات أمن المعلومات Information security Tools: أدوات وآليات متبعة للحفاظ على المعلومات والبيانات المتداولة عبر الإنترنت من العبث والتخريب، من خلال وسائل حمايتها من المخاطر الداخلية والخارجية
22. استرجاع / استعادة البيانات Data recovery: هي عملية لإنقاذ البيانات التي لا يمكن الوصول إليها من مخزن البيانات الثانوي التالف أو من الوسائط المتعددة.
23. سلامة البيانات Data integrity : بياناتك ومعلوماتك الشخصية أمر مهم يجب الحفاظ عليه وحمايته من الهجمات التخريبية أو السرقة.
24. سرية المعلومات Information confidentiality: هي التحكم في الدخول إلى البيانات وإتاحتها، بمعنى تحديد الفئات المعنية المسموح لها بالاطلاع على البيانات.
25. التشفير Encryption: عبارة عن ضمان أمن المعلومات باستخدام الخوارزميات المشفرة وعلامات التجزئة والتوقيعات.
26. التوقيع الرقمي Digital Signature: تُعد أنظمة التوقيع الرقمي نوعاً من التشفير العام للبيانات؛ فمن خلال استخدام مفتاح خاص يتم التأكد من سلامة البيانات ومصادقتها وعدم إنكارها.





27. رمز مُصادقة الرسائل (MAC): باستخدامه يَشترك طرفان أو أكثر في مفتاح. يُنشئ أحد الأطراف علامة رمز المُصادقة ويُرفقها بالمستند. ويستطيع الآخر التَّحَقُّق من سلامة الرِّسالة عبر المفتاح نفسه.

28. الحوسبة التَّشفيريَّة Cryptographic computing: يُغطِّي المصطلح مجموعة كبيرة من التَّقنيَّات، بما فيها الحوسبة الآمنة مُتعدِّدة الأطراف والتَّشفير التَّماثلي والتَّشفير القابل للبحث.

29. مخترق الأجهزة والبيانات Hacker: شخص ذو إمكانيَّات برمجية وتقنية عالية تُعطيه القدرة على استغلال الثَّغرات الأمنيَّة في البرامج والأنظمة والمواقع الإلكترونيَّة؛ لأهدافٍ مختلفة.

30. المُمارسات التَّكنولوجيَّة الآمنة Safe technology practices: أُوجِّدَت التَّكنولوجيا ومواقع التَّواصل الاجتماعيَّ نوعًا جديدًا من الممارسات الفرديَّة، والتي تتنوع بين الإيجابيَّة والسَّليبيَّة.

31. الحرب الإلكترونيَّة E-war: مجموعة الإجراءات المُستخدَمة في الحروب التَّقليديَّة، تتضمَّن استخدام نُظم إلكترونيَّة حديقة في استطلاع الإشعاع الكهرومغناطيسيِّ الصَّادر من نُظم العدوِّ ووسائله.

32. المرجع الإلكتروني Electronic reference: هو عملية توفير المعلومات المطلوبة للهجوم الإلكتروني أو الحماية الإلكترونية.

33. الإرهاب السيبراني Cyber terrorism : هو استخدام التقنيات الإلكترونية والرقمية لإلحاق الأذى أو إخافة وإخضاع الآخرين أو مهاجمة نظم المعلومات للأفراد والمؤسسات.

34. برمجيات التعقب Stalker ware: هي أحد أنواع التقنيات التي تسمح لشخص ما بمراقبة والتجسس على شخص آخر من خلال تنصيب تطبيق أو برمجية على هاتفهم أو حاسبهم دون علمهم

35. إدارة المخاطر الرقمية Digital Risks Management: هي تنفيذ العمليات الرقمية التي تهدف لتوفير الدعم اللازم لضمان استمرارية الأعمال وتحسين تقييم المخاطر.

36. الثغرات الأمنية Security vulnerabilities: هي نقطة ضعف أو غيب أو خطأ يتم العثور عليه داخل أنظمة الحاسوب والشبكات، يمكن أن يتم الاستفادة منه من قبل المخترقين لاختراق شبكة آمنة.



37. إدارة الثغرات الأمنية Security vulnerabilities management: هي عملية مُستمرة واستباقية وغالبًا ما تكون تلقائية، تُحافظ على أمان أنظمة الحاسوب والشبكات وتطبيقات المؤسسة ضد الهجمات عبر الإنترنت وعمليات خرق البيانات.

38. اختبار الاختراق Penetration testing: برنامج يساعد مُتخصصي تكنولوجيا المعلومات في العثور على الثغرات الأمنية في أنظمة الحاسوب واستغلالها.

39. التحليل الذكي للمخاطر Intelligent risk analysis: هو برنامج حماية من المخاطر يوفر للمؤسسات القدرة على تتبع المخاطر المحتملة ومراقبتها وتحليلها وتحديد أولوياتها لحماية نفسها بشكل أفضل.

40. أنواع المعلومات Information Types: يمكن أن تكون المعلومات غير نشطة (مثل: ملف على القرص الصلب)، أو متحركة (مثل: الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر)، أو قيد الاستخدام (أثناء الحوسبة على البيانات).

41. رسائل التسويق المضللة Misleading marketing messages: رسائل يُرسلها المُخترقون عبر الهواتف الذكية في إطار تسويق منتجات وخدمات، لكنها تهدف لاختراق هذه الأجهزة وسرقة البيانات.

42. التحقق من الهوية Identity verification: هي عملية تأكيد هوية شخص ما. قد تستخدم عملية التحقق طرقًا مختلفة، بما في ذلك طلب تحديد هوية صادر عن الحكومة.

43. التحقق من الهوية الرقمية Digital identity verification: تأكيد الهوية الرقمية لشخص ما من خلال الإنترنت. مثل: التحقق من قواعد البيانات الحكومية وملفات تعريف وسائل التواصل الاجتماعي.

44. القرصنة الإلكترونية Electronic piracy: اختراق لأجهزة الحاسوب عبر شبكة الإنترنت، ويقوم بهذه العملية شخص أو مجموعة أشخاص لديهم خبرة واسعة في برامج الحاسوب والتعرف على محتوياته.

45. سرقة النقر clickjacking: هجمات تُخدع المُستخدم للنقر فوق عُنصر صفحة ويب غير مرئي أو يتخفى كعنصر آخر، ويتسبب ذلك في تنزيل المُستخدمين برمجيات ضارة عن غير قصد.

46. سرقات "الإعجاب" Like jacking: في هذا الهجوم يتم خداع المُستخدمين للنقر على زر "أعجبني" على Facebook، حيث يحتاج المُستخدم لتسجيل الدخول للموقع عند النقر على الرابط لنجاح الهجوم.

47. سرقة المؤشر cursor jacking: يتم إنشاء مؤشر مكرّر وإرفاقه بالمؤشر الحقيقي عند إزاحة مُحَدَّدة، حيث يكون المؤشر المكرّر فقط مرئيًا، بحيث يتم النقر فوق ارتباط ضار عند المناورة بالمؤشر الوهمي.

48. سياسة أمان المحتوى (CSP) Content Security Policy: آلية للكشف والوقاية، تُستخدم للحد من الهجمات الإلكترونية، مثل: XSS و click jacking.

49. هجوم دون تفاعل المستخدم Zero-Click Attack: هجوم عن بُعد على جهاز ما، لا يتطلب أي إجراءات إضافية من المستخدم. يمكن تنفيذه عن طريق الجوّ (OTA عبر الهواء).

50. الابتزاز الإلكتروني Electronic blackmail: يُعتبر الابتزاز الإلكتروني عامِل تهديد للأفراد من خلال نشر معلومات حسّاسة عبر الإنترنت إذا لم يلتزموا بتنفيذ مطالب المهاجمين من جهةٍ ما.

51. صناعة المحتوى المزيف Generating fake content: يمكن للذكاء الاصطناعي إنشاء محتوى مزيف يبدو كأنه تمّ توليده من الضحية نفسها. قد يكون رسائل نصّية أو إلكترونية تتضمن معلومات خادعة.

52. تهديدات التشهير Threats of Publish: من خلال الذكاء الاصطناعي يمكن توليد رسائل تهديد تحاكي لغة الضحية؛ حيث يُهدّد المُجرِّمون بنشر معلومات حسّاسة على وسائل التواصل الاجتماعي إذا لم يتمّ تلبية مطالبهم.

53. التجسس والمراقبة Espionage and surveillance: مراقبة الذكاء الاصطناعي لنشاطات الضحية عبر الإنترنت ومواقع التواصل الاجتماعي واستخدام هذه المعلومات لابتزازهم.

54. التلاعب بالمعلومات Information manipulation: يستطيع الذكاء الاصطناعي التلاعب بالمعلومات عبر الإنترنت مثل: تغيير الصور أو تعديل الرسائل بطريقة تجعلها تبدو وكأنّها من الضحية نفسها.

55. استغلال التقنيات الصوتية والرُّسوم المتحركة Exploiting audio and animation techniques: توليد مقاطع صوتية ورُّسوم متحركة مُزيّفة تبدو وكأنّها من الضحية المُتورّطة في سلوك غير لائق.

56. التفاعل مع الضحايا Interacting with victims: عبر تصميم سيناريوهات مُحادّثة تفاعلية مع الضحايا، وتشغيل دردشات آلية تهدف لجمع معلومات أو مطالبة الضحية بتلبية بعض المتطلبات.

57. خرق البيانات الشخصية Personal data breach: هو سرقة معلومات حساسة أو تسريبها من قبل فرد أو منظمة أو مجموعة من قرصنة المعلومات الذين يبحثون عنها.

58. تفعيل التحقق متعدد العوامل Multi-Factor Authentication (MFA): طريقة تصديق تتطلب وسيلتين أو أكثر من عوامل التحقق -كلمات المرور أو بصمة الإصبع- للسماح بولوج المصدر، كتطبيق ما أو حساب على أحد المواقع.

59. الحوسبة السحابية: Cloud computing: مصطلح يشير للمصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة، والتي تستطيع توفير خدمات حاسوبية متكاملة دون التقيد بالموارد المحلية.

60. تصعيد/ترقية الصلاحيات Escalation privilege: يشير المصطلح لمهاجم تمكن من اختراق حساب أو أكثر، ويعمل على الاستفادة من تلك الامتيازات المحدودة للحصول على إمكانية الدخول إلى حسابات ذات امتيازات أكبر.

61. الانتحال Impersonation: تزيف رأس الرسالة الإلكترونية بواسطة مهاجم لكي تبدو الرسالة صادرة من شخص آخر غير المصدر الحقيقي.

62. تزيف البريد الإلكتروني Email spoofing: تكتيك يُستخدم في التصيد الاحتيالي؛ لأنّ مُستخدمي البريد الإلكتروني غالباً ما يفتحون الرسالة إذا اعتقدوا أنّها من مصدر قانوني موثوق به.

63. الهندسة الاجتماعية Social engineering: هي ليست هجوماً إلكترونياً، بل تدور حول كسب ثقة الأشخاص وإقناعهم بالتخلي عن حذرهم، وتشجيعهم على اتخاذ إجراءات غير آمنة؛ مثل إفشاء المعلومات الشخصية.

64. الفضاء السيبراني Cyberspace: هو وسط عالمي يتألف من مكونات مادية مثل الحواسيب وشبكات الاتصال والبنى التحتية الرقمية ومستخدمي الإنترنت، ومكونات لا مادية مثل البرامج والنظم الحاسوبية ونظم الاتصال.

65. هجمات خرق البريد الإلكتروني للعمل Business Email Compromise (BEC) Attacks: شكل من أشكال احتيال البريد الإلكتروني؛ حيث يدّعي المهاجم أنّه أحد كبار المديرين التنفيذيين، ويحاول خداع المُستلم لينفذ مهام عمله، لهدف غير قانوني.

66. الاصطياد عبر USB (USB Baiting): من خلاله ينصب المجرمون الإلكترونيون برمجيات ضارة على أقراص USB ويتركونها في مواقع إستراتيجية، فيستخدمها أحد ما، وبالتالي يصبح عُرضة لأكواد ضارة مُتعددة.

67. الخصوصية Privacy: هي قدرة الفرد أو الأشخاص على عزل أنفسهم ومنع المعلومات المتعلقة بهم لتصبح معروفة للآخرين، وبالأخص المنظمات والمؤسسات.

68. التَّجَسُّس على حَرَم البيانات Data packet sniffing: تُراقب هذه الهجمات حركة المرور باستخدام تطبيق أو جهاز، ويجعل حركة مرور الويب الخاصة بالضحية عرضة لمُجرمي الإنترنت.

69. كسر شفرة طبقات أمان النقل SSL BEAST: يصيب القرصنة جهاز حاسوب المُستخدم بجافا سكريبت ضار. ثمّ تعترض البرمجيات الضارة مِلَفات تعريف الارتباط الخاصة بموقع الويب ورؤوس المصادقة المُميّزة لفك التشفير.

70. مِلَفات تعريف الارتباط للمتصفح Browser cookies: أجزاء مُفيدة من معلومات موقع الويب التي تُخزنها المواقع التي يزورها المُستخدم، وتُساعد في تذكُّر نشاط الويب وعمليات تسجيل الدُّخول.

71. تجريد أمان طبقة النقل SSL Stripping: يعترض مُجرم الإنترنت إشارة أمان طبقة النقل (TLS) من التطبيق أو موقع الويب ويُعدّلها ليتِم تحميل الموقع على اتصال غير آمن في صورة HTTP عَوَضًا عن أن يكون HTTPS.

72. تزوير حَرَم البيانات Forging packages: يُنشئ مُجرم الإنترنت حَرَمًا تبدو طبيعيّة، ويقوم بضحّها في شبكة قائمة للوصول إلى حركة البيانات ورصدها أو لشنّ هجمات الحرمان من الخدمات المُوزَّعة (DDoS).

ثالثًا: عدد 8 بطاقات أمن سيبرانيّ Cybersecurity- 2 من كل لون، هذه البطاقة تُعطي الحقّ لمالكها في الحصول على ثلاثة اختيارات لعنوان الموضوع يُختار منها إجابة واحدة فقط لمرة واحدة فقط.

رابعًا: عدد 8 بطاقات جريمة اختيال Fraud Crime- 2 من كل لون، تلك البطاقة تُساعد مَالِكها في التّحايّل على الإجابة عن عنوان البطاقة، وأن يكون الطّالب التّالي له مُطالبًا بالإجابة بدلًا منه.

خامسًا: عدد 4 بطاقات من جريمة سرقة البيانات Data Theft، وتلك البطاقات تُعطي الطّالب الحقّ في الحصول على البطاقة محلّ التّخمين من صاحبها، وأن يختار 3 طُلاب للإجابة عن عنوان البطاقة، ويعاقب صاحب الإجابة الخاطئة بسحب بطاقتين.

سادسًا: عدد 4 بطاقات من خرق البيانات Data Breach، وفيها يطلب الطّالب من طالب آخر مُحدّد الإجابة بدلًا منه أو سحب 3 بطاقات. وفي حالة الإجابة الخاطئة يسحب 4 بطاقات.

سابعًا: عدد 8 بطاقات 2- من كل لون- من خرق البنية التّحتيّة Infrastructure Breach، وتلك البطاقات تُؤدّي إلى إنهاء دَوْرَة اللعب بشكل قوْريّ، وبدء دَوْرَة جديدة لكن بشرط البدء من آخر قَرْد في الدّورة السّابقة.

ثامنًا: عدد 8 بطاقات 2- من كل لون- من التّنمّر الإلكترونيّ Cyberbullying، وتلك البطاقات تُجعل مَالِكها يختار بطاقة من البطاقات التي يملكها، وأن يُطلب من الطّالب صاحب البطاقة الأولى محلّ التّخمين أن يُجيب هو عنها، وفي حال الإجابة الخاطئة يسحب 3 بطاقات.

طريقة اللعب

- اللُّعبة لا بُدَّ أن تكون مُكوَّنة من طالبيين أو أكثر يمكن أن يصل عدد الطَّلَبَة إلى 6 أفراد.
- أقل سنٍ يمكنه المُشاركة في اللُّعبة (17 سنة).
- في بداية اللُّعبة يحصل كلُّ طَالِبٍ على عدد 7 بطاقات، وباقي البطاقات تُوضع في الجانب للسَّحب منها أثناء اللُّعب.
- تبدأ اللُّعبة دائماً بعد ترتيب البطاقات بطريقة عشوائية، وتوزيع 7 بطاقات على كلِّ طَالِبٍ، ويبدأ اللُّعب الطَالِب الذي يجلس في الناحية اليمنى من مُوزِّع البطاقات.
- يختار الطَالِب بطاقة واحدة من البطاقات التي يملكها، ويبدأ في شَرْح المُصطلح الذي يُعبّر عن موضوع البطاقة، دون أن يَذكر عنوان البطاقة.
- على الطَالِب التَّالي له أن يخمّن عنوان البطاقة.. وله مُحاولة واحدة فقط للتَّخمين.
- إذا أجاب الطَالِب التَّالي إجابةً صحيحةً؛ فإنَّ الأوَّل يضع البطاقة على الطاولة، ويسحب بطاقة أخرى من البطاقات الموضوعة جانباً.. أمَّا الطَالِب التَّالث فيسحب بطاقة واحدة من البطاقات المملوكة للتَّاني.
- إذا أجاب الطَالِب التَّاني إجابةً خاطئةً يَسحب بطاقتين من البطاقات الموضوعة جانباً.. ويكون الدَّور على التَّالث أن يخمّن عنوان البطاقة.
- إذا أجاب الطَالِب التَّالث إجابةً صحيحةً؛ فإنَّ الأوَّل يضع البطاقة على الطاولة، ويسحب بطاقتين من البطاقات الموضوعة جانباً.. أمَّا الطَالِب الرَّابع فيسحب بطاقة من بطاقات الطَالِب التَّالث.
- وإذا أجاب الطَالِب التَّالث إجابةً خاطئةً يَسحب 3 ورقات من البطاقات الموضوعة جانباً.. ويكون الدَّور على الطَالِب الرَّابع أن يخمّن عنوان البطاقة.
- تسير اللُّعبة على هذا المنوال حتى اكتمال دَوْرَة كاملة، ثُمَّ البدء من جديد بطاقة أخرى جديدة.
- إن كان الطَالِب معه بطاقة واحدة فقط لينتهي من بطاقاته؛ فعليه أن يقول Last card قبل أن يَنْتقل الدَّور للفرْد التَّالي، وإلاَّ تَتِمَّ مُعاقبته بِسحب 6 بطاقات من البطاقات الخاصَّة بالسَّحب.
- وخلال اللُّعب على كلِّ طالب مُحاولة التَّخلُّص من البطاقات التي يَمْتَلِكها، ومع إلقاء آخر بطاقة لَعِب لا بدَّ أن يقول الطَالِب: سيبرونو.. ويكون هو الفائز الأوَّل.

قوانين اللعبة

- إذا كان الطالب يملك بطاقة آمن سيراني؛ فإنه يطلب ثلاثة اختيارات لعنوان البطاقة محلّ التخمين، كي يختار منها إجابة واحدة فقط لمرة واحدة فقط.
- إذا كان الطالب يملك بطاقة جريمة اختيال، فيمكنه التّحايّل على الإجابة عن عنوان البطاقة، وأن يكون الطالب التّالي له مُطالبًا بالإجابة بدلًا منه.
- إذا كان الطالب يملك بطاقة جريمة سرقة البيانات، فيمكنه الحصول على البطاقة محلّ التخمين من صاحبها، وأن يختار 3 طلبة للإجابة عن عنوان البطاقة، ويُعاقب صاحب الإجابة الخاطئة منهم بسحب بطاقتين.
- إذا كان الطالب يملك بطاقة خرق البيانات، فيمكنه أن يطلب من طالب آخر مُحدّد الإجابة عن عنوان البطاقة بدلًا منه أو يسحب 3 بطاقات. وفي حالة الإجابة الخاطئة يسحب 4 بطاقات.
- إذا كان الطالب يملك بطاقة خرق البنية التحتية، فيمكنه إنهاء دورة اللعب بشكّل قووي، وبدء دورة جديدة، لكن بشرط البدء من آخر قرّد في الدورة السابقة.
- إذا كان الطالب يملك بطاقة التّمر عبر الانترنت؛ فإنه يختار بطاقة من البطاقات التي يملكها، ويطلب من الطالب صاحب البطاقة الأولى محلّ التخمين أن يجيب هو عنها، وفي حال الإجابة الخاطئة يسحب 3 بطاقات.

- وتتوالى الأدوار بين باقي الطلبة حتّى يُصبح آخر طالب هو الخاسر.
- وفي حالة انتهت البطاقات الاحتياطية الخاصة بالسحب، ولا يزال يُوجد أكثر من طالب؛ يقوم مُورّع اللعبة بإيقاف اللعبة مؤقتًا، ويبدأ في إعادة ترتيب البطاقات من جديد، ومن ثمّ يضعها من جديد كبطاقات احتياطية يمكن للطلبة السحب منها.







اللّعبة الرّابِعة: Cyber Way

فكرة اللعبة

تقوم فكرة اللعبة على إجراء مسابقات معرفية حول الأمن السيبراني بين الطلبة، وتجمع اللعبة بين التحدي والمنافسة والمعرفة والتسلية، فهي تقدم معلومات، وتختبر المخزون المعرفي للطلبة ضمن إطار تنافسي قائم على المنافسة والتسلية.

تتألف اللعبة من رُقعة مُقسّمة إلى مَرَبَّعات صغيرة تصل إلى 100 خانة، لها بداية ونهاية، والمَرَبَّعات ملوّنة بألوان مختلفة، ولكلّ طَالِب مُجَسَّم خاصّ به يَضَعه على اللّوح، ويأتي مع اللعبة حجر نرد، يتم رميه، وتحريك المُجَسَّم الخاصّ بكلّ طَالِب إلى مَرَبَّعات بعدد النّقاط التي تظهر على حجر النرد.

تبدأ اللعبة برمي الطلبة حجر النرد، وصاحب الرّقم الأعلى يبدأ أولاً، ومن بعده الطّالِب الَّذِي حَصَلَ على نقاط أقلّ، ونزول الطّالِب على أيّ خانة يُعطي فارقاً مُميّزاً بالنّقلات.

والواصل أولاً إلى المَرَبَّع رقم 100 هو الرّابح.

السن المناسبة للعبة

15+ سنة

تسمية اللعبة

اسم اللعبة Cyber Way يتألف من شقين: الأول ساير Cyber، ويشير إلى البيئة السيبرانية. والثاني Way، ويُقصد به الطريق أو المسار، وبذلك يصبح اسم اللعبة الطريق أو المسار السيبراني، وهو ما يتقاطع مع جوهر اللعبة، والذي يتعلق بمسار يسلكه الطالب يبدأ من المربع رقم (1)، وينتهي في المربع رقم (100).

النقاط المميّزة في اللعبة

تقتضي اللعبة وجود ثلاثة فرق ملوّنة نسبةً إلى قُبَعات الهاكرز المعروفة.

1. الفريق الأحمر Red Team

وهو فريق هجوميّ، يهدف لتنفيذ هجمات افتراضية على الأنظمة والبنى التحتية الرقمية في المؤسسات، ويسعى لاختراق هذه النظم، ولكن ليس بهدف الإضرار بها، بل بهدف تحديد إمكانيّة اختراقها، وفي حال التمكن من الاختراق؛ فهذا يعني أنّ نظم الحماية في المؤسسة ضعيفة ولا تستطيع مواجهة الهجمات الإلكترونية.

2. الفريق الأزرق Blue Team

فريق متخصص في الأمن السيبرانيّ، لكنّه فريق دفاعيّ مهمته الأساسية تحصين المؤسسة من الاختراقات، تقع عليه مسؤولية التعامل مع البيانات والأجهزة والبنية التحتية وحمايتها.

3. الفريق الأرجواني Purple Team

مشتق من الفريقين الأزرق والأحمر، يعتمد في عمله على نتائج عمل كلّ من الفريقين الأحمر والأزرق، فهو يقوم بإعداد قائمة بنقاط الضعف والثغرات التي تمكّن الفريق الأحمر من إيجادها، ويقدمها للفريق الأزرق ليقوم بتزميم وإصلاح نظم الدفاع السيبرانيّ الخاصة بهذه الثغرات.

مكوّنات اللعبة

1. لوح اللعبة الرئيس: وهو مقسم لمربعات تأخذ أرقامًا من 1-100، مربعات اللوح ملوّنة بحسب ألوان القُبَعات؛ وضمن بعض مربعات اللوح يوجد أشكال، تُقسّم لقسمين؛ أشكال ترمز للأمان الرقميّ، وأخرى للخطر، والأشكال التي ترمز للأمان هي رمز الدرع والمفتاح، والتي ترمز للخطر هي رمز القنكبوت والجُمجمة.
2. مجسمات مختلفة الأشكال، ومقسّمة إلى 3 ألوان بحسب ألوان القُبَعات، يتم توزيعها على الطلبة عند بدء اللعب.
3. حجر نرد لتحديد ترتيب الطلبة في اللعب، ولتحريك المجسمات على اللوحة.
4. 90 بطاقة سؤال (30 بطاقة لكل لون).
5. فلاير يضم إجابات الأسئلة التي تحتوي عليها البطاقات.

أنواع المُربَّعات

مُربَّعات اللّوح مُلوّنة بحسب ألوان القُبَّعات.. عند رَمي النّرد يتحرّك الفريق الأزرق ضَمَن خاناته الرّزقاء بشكلٍ عاديّ، لكنّ عند وقوفه على أحد مُربَّعات فِرَق القُبَّعات الثّانية، سيكون مُضطرباً للإجابة عن أسئلة الفريق الثّاني باعتباره استأجر خانةً من خاناتها، وإذا فشل في الإجابة سيَعُود لمُربَّعه السّابق قبل رَمي حَجَر النّرد.

• المُربَّعات الرّزقاء:

ستكون أسئلتها خاصّة بمفاهيم مُتقدّمة في الأمن السيبرانيّ ذات طابع دفاعيّ مثل: (تحليل البصمة الرّقميّة- عمليّات تدقيق DNS، مُراقبة نشاط الشّبكة، استخدام الوصول الأقلّ امتيازاً، تقنيات التّعزيز، تحليل البرمجيّات الضّارة، أنظمة التّشفيل، الطّبّ الشرعيّ الرّقميّ، الاستجابة للحوادث).

• المُربَّعات الحمراء:

خاصّة بمفاهيم مُتقدّمة خاصّة ذات طابع هجوميّ مثل: (اختبار الاختراق، اعتراض الاتّصالات، الهندسة الاجتماعيّة، تطوير البرمجيّات، الأمن الماديّ).

• المُربَّعات الأرجوانيّة:

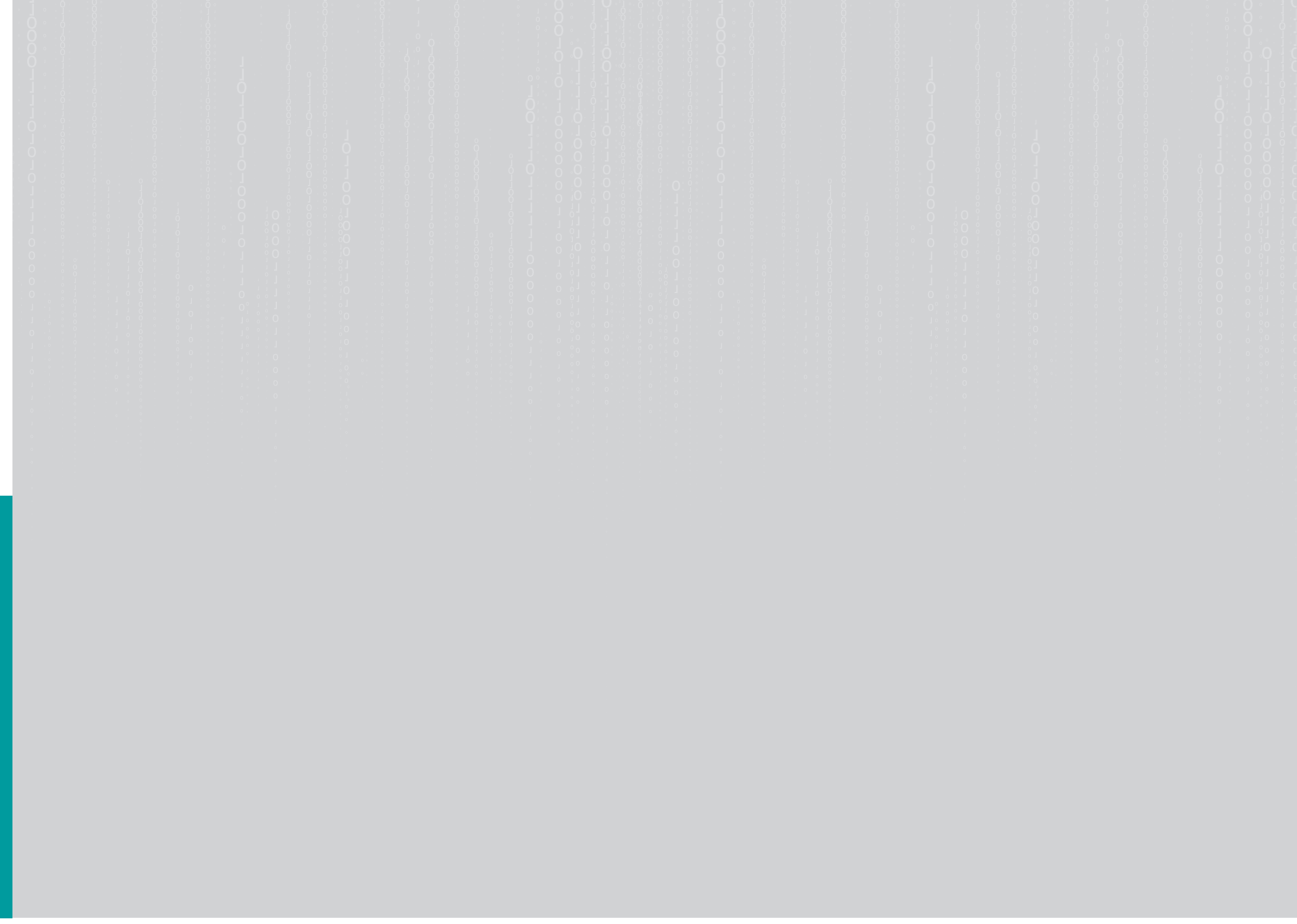
خاصّة بأكثر المخاطر السيبرانيّة شدّة (نشر أنشطة كُشف/ منع التّسلّل، مُراقبة حركة مرور الشّبكة بحثاً عن أيّ نشاط مشبّوه، عمليّات فحص مُنظمة الثّغرات الأمنيّة، وُضع وتنفيذ خطة أمنيّة شاملة، إطلاق هجمات البرمجيّات الضّارة والأخطاء السيبرانيّة ضد الأنظمة الحيويّة، تنفيذ هجمات الهندسة الاجتماعيّة، ومحاولة الوصول إلى البيانات الحسّاسة، تحديد وتصحيح الثّغرات الأمنيّة).



طريقة اللعبة

1. تعتمد اللعبة على الأداء الجماعي، ويمكن بدء اللعب بحد أدنى 3 طلبة.
2. يتم تقسيم مجموعة الطلبة إلى 3 فرق؛ بحسب ألوان القبعات.
3. يختار كل طالب مجسمًا محددًا يكون فريقه للتحرّك به على لوح اللعب.
4. يقوم كل طالب برمي حجر النرد، والطالب الحاصل على الرقم الأكبر يبدأ جولة اللعب، ومن بعده الطالب الذي حصل على نقاط أقل.
5. عند وجود مجسم أحد الطلبة على مربّع ذي لون مماثل للون فريقه يسيّر اللاعب بشكل طبيعي، فعلى سبيل المثال: إذا كان مجسم الفريق الأزرق على مربّع ذي لون أزرق؛ فهذا الأمر لا يترتب عليه أي تبعات، ولكن إذا كان مجسمه على مربّع ذي لون مغاير للون فريقه، سيكون مضطرًا للإجابة عن أسئلة الفريق ذي اللون المماثل للون المربّع، فإذا كان مجسم الفريق الأزرق على مربّع ذي لون أحمر، فعلى الفريق الأزرق حينها الإجابة عن سؤال يطرحه عليه الفريق الأحمر، وإذا فشل الطالب أو أحد أعضاء فريقه في الإجابة سيغود الطالب لمربّعه السابق قبل رمي حجر النرد، أمّا إذا أجاب الطالب أو أحد أعضاء فريقه إجابة صحيحة فسينتقل مربّعًا إلى الأمام، وبالمثل باقي الطلبة.

6. في حال كان مجسم أحد الطلبة على مربّع يحوي رمز الدرع يتم نقل مجسمه مربّعًا إلى الأمام، وفي حال كان على مربّع يحوي رمز المفتاح يتم نقل المجسم مربّعين إلى الأمام، فرموز الدرع والمفتاح تساعد الطلبة في التّقدّم إلى الأمام، (في حال نقل مجسم الطالب إلى الأمام مربّعًا أو مربّعين لن يكون مضطرًا للإجابة عن أي أسئلة في حال جاء مجسمه على لون مخالف للون فريقه، وذلك على اعتبار أنّه أجاب عن أسئلة الفرق الأخرى في الخطوة السابقة).
7. في حال كان مجسم أحد الطلبة على مربّع يحوي رمز القنكبوت يتم نقل مجسمه مربّعًا إلى الخلف، وفي حال كان على مربّع يحوي رمز الجمجمة يتم نقل المجسم مربّعين إلى الخلف، فرموز القنكبوت والجمجمة تعيد الطلبة إلى الوراء، (في حال نقل مجسم الطالب إلى الأمام مربّعًا أو مربّعين لن يكون مضطرًا للإجابة عن أي أسئلة في حال جاء مجسمه على لون مخالف للون فريقه، وذلك على اعتبار أنّه أجاب عن أسئلة الفرق الأخرى في الخطوة السابقة).
8. تتوالى اللعبة على هذا المنوال، والطالب الواصل أولًا إلى المربّع رقم 100 يكون فريقه الرّابح.
9. في حال انتهت كلّ الأسئلة، ولم يكن أحد الطلبة قد وصل للمربّع رقم 100، يتم إيقاف اللعبة، ويكون الفائز هو الطالب الذي يكون مجسمه في المربّع الأقرب للرقم 100.





اللّعبة الخامسة لعبة الأفكار التعليمية

فكرة اللعبة

لُعبة توعويّة تعليميّة للطلّبة الصّغار تستخدم طريقة الألوان والرُّسوم والتّلوين، وتهدف إلى تعريفهم برُّموز المفاهيم العامّة ذات الصّلة بالأمن السيبرانيّ والسّلامة الرّقميّة، عبر خطواتٍ بسيطةٍ يسهّل استيعابها خلال هذه السّنّ الصّغيرة بطريقةٍ مُمتعةٍ. كما تهدف اللّعبة إلى إحداث تأثيرٍ توعويٍّ إيجابيّ طويل المدى في ترسيخ مبادئ السّلامة الرّقميّة؛ من خلال نشاط ترفيهيّ اجتماعيّ مُمتع بين المُعلّمين والطلّبة داخل الصّف الدّراسيّ وخلال فترات الاستراحة، أو مع أولياء أُمورهم في المنزل.

أهداف اللعبة

1. تعليم الطّلبة الصّغار مُصطلحات وأفكار سيبرانيّة جديدة ومُبسّطة.
2. تنمية المهارات اللّغويّة والمعرفيّة في المجال السيبرانيّ للطلّبة.
3. ترسيخ الأسس المعرفيّة في المجال المعلوماتيّ لدى الطّلبة الصّغار؛ من خلال المرّج بين التّرفيه والتّنافس والتّعلّم.
4. تزويد الطّلبة بجرّعة من المُثقة والتّسلية، والشّعور بالإنجاز عن طريق مُسابقات تفاعليّة مُتنوّعة.

العمر المُخصّص للعبة

4-6 سنوات (المرحلة الابتدائيّة)

مكوّنات اللعبة

1. 60 بطاقة مُسابقات في 10 موضوعات سيبرانيّة وتكنولوجيّة رئيسة (6 بطاقات مُلوّنة بلّون واحد لكلّ موضوع).
2. لوح اللّعب.
3. كُتيّب للإجابات.
4. دليل اللّعبة.



آلية اللعب

1. اللّعبة تعتمد على الأداء الفردي، فيمكن أن تكون بطالين أو أكثر، فيتنافس كلّ طالب مع باقي زملائه على الإجابة عن أكبر قدر ممكن من الأسئلة.
2. يقوم أحد الطّلبة/ الوالدين بدور الحَكَم لتوزيع البطاقات على الطّلبة، وتقييم الإجابات من الكُتيب الخاصّ بها.
3. في البداية، يقوم الحَكَم بخلط البطاقات بشكلٍ عشوائيٍّ، ووضْعها على لوح اللّعب.
4. تبدأ الدّورة الأولى من اللّعب بقيام كلّ طالب باختيار بطاقة واحدة بشكلٍ عشوائيٍّ من البطاقات، دون رؤية الأسئلة.
5. بعد ذلك يبدأ الجميع في الإجابة عن الأسئلة الموجودة في بطاقتهم في الوقت ذاته، كلٌّ بمفرده ودون الاستعانة بأحدٍ.
6. الطالب الفائز في الدّورة الأولى من اللّعب هو الذي يُجيب أولاً عن السؤال الخاصّ به، لكنّ يشترط أن تكون الإجابة صحيحة.
7. بعد انتهاء جميع الطّلبة من حلّ السؤال الأول، يجمع الحَكَم البطاقات المُستخدَمة، ويضعها في المكان المُخصّص لها على لوح اللّعب.
8. يبدأ الطّلبة لعب دّورة جديدة ببطاقات أخرى جديدة وبالطريقة السابقة ذاتها.

9. يسير اللّعب على هذا المنوال حتّى اكتمال استخدام كلّ البطاقات أو لحين يُقرّر الجميع إنهاء اللّعب.
10. يُخصي الحَكَم عدد الدّورات التي فاز بها كلّ طالب، والفائز في النّهاية هو الفائز بأكثر دورات اللّعب عدداً. فإذا استطاع طالب الفوز بـ 5 دورات، وهو العدد الأكبر بين زملائه، يكون هو الفائز.

أسس تقييم أداء الطلبة في الألعاب التدريبية

للألعاب التدريبية عدة أهداف؛ أهمها الأهداف التدريبية والتقييمية؛ فمن خلال أداء الطلبة في الألعاب، من الممكن إجراء تقييم أولي لمدى الاستفادة من المحتوى التدريبي والتوعوي الذي تم تقديمه لهم خلال الورش التدريبية؛ فمقدرة الطالب على التقدم في الألعاب والفوز بها يعتمد بشكل رئيس على مخزونه المعرفي في مجال الأمن السيبراني؛ لذلك فالطلبة القادرون على الوصول لمراحل متقدمة في الألعاب، والفوز بها يعدون محققين نسبة مرتفعة من الفائدة المعرفية من الورش التدريبية، والعكس صحيح.

لذلك، وعند قيام الطلبة باللعب، لا بُدَّ للمدرب من تقييم أداء الطلبة، من خلال جدول يُنظَّم مسبقاً، يتم به تسجيل نوع اللعبة، وأسماء الطلبة اللاعبين في دور واحد، وإزاء كل طالب يقوم المدرب بتسجيل ملاحظاته على أداء كل طالب؛ وفيما يلي تبيان لتفاصيل بطاقات التقييم الجماعية المخصصة للألعاب التدريبية.

اسم اللعبة						
المرحلة التعليمية:				اسم المدرب:		
مسلسل	اسم الطالب	معايير التقييم				ملاحظات المدرب
		درجة الانسجام مع زملائه	فهم اللعبة وإدراك قواعدها	القدرة على التقدم في اللعبة	القدرة على الإجابة عن أسئلة اللعبة	القدرة على الاستفادة من الورش التدريبية في التعامل مع اللعبة
1						
2						
3						
4						



وبخصوص نقاط التقييم؛ فوفقاً للمنهجيات العلمية المعتمدة في هذا المجال، فكلما ازداد عدد درجات سلم التقييم؛ انعكس ذلك إيجاباً على دقة عملية التقييم ومطابقتها للواقع، فالبطاقة تعتمد سلباً من أربع درجات، فيما يلي تبيان له ولكيفية وضع تقييم الطلبة في كل محور من محاور البطاقة.

المؤشر	دلالة المؤشر	رمز المؤشر	دلالة المؤشر	رمز المؤشر	دلالة المؤشر	رمز المؤشر	دلالة المؤشر
درجة الانسجام مع زملائه	غير منسجم أبدًا	(-)	منسجم بشكل متوسط	(+)	منسجم بالحدود الدنيا	(-)	(+ + +)
فهم اللعبة وإدراك قواعدها	لم يفهم اللعبة أبدًا	(-)	فهم متوسط للعبة	(+)	فهم مقبول للعبة	(-)	(+ +)
القدرة على التقدم في اللعبة	غير قادر على التقدم في اللعبة	(-)	قادر بشكل متوسط على التقدم في اللعبة	(+)	قادر بشكل بسيط على التقدم في اللعبة	(-)	(+ + +)
القدرة على الإجابة عن أسئلة اللعبة	غير قادر على الإجابة عن أسئلة اللعبة	(- -)	قادر بشكل متوسط على الإجابة عن أسئلة اللعبة	(-)	قادر بشكل بسيط على الإجابة عن أسئلة اللعبة	(- -)	(+ +)
القدرة على الاستفادة من الورش التدريبية في التعامل مع اللعبة	لم يظهر قدرة على الاستفادة من الورش التدريبية في اللعبة	(- -)	أظهر قدرة متوسطة على الاستفادة من الورش التدريبية في اللعبة	(-)	أظهر قدرة بسيطة على الاستفادة من الورش التدريبية في اللعبة	(- -)	(+ +)

وفقًا لجداول الترميز أعلاه، فعندما يلاحظ المدرب أحد الطلبة بأنه منسجم بشكل متوسط، يضع له إشارة (+ +)، وهكذا لبقية التقييمات، والتي مقابل كل منها تم وضع ترميزها.

