



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 المُبتكرة 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

7	تمهيد
9	المِخْوَْر الأوّل: مشروع سايبر إيكو
11	• نظرة عامّة على المشروع
12	• دلالة اسم المشروع
12	• الفئات المُستهدّفة بالمشروع
12	• رؤية المشروع
12	• رسالة المشروع
13	• أهداف المشروع
13	• أهمّيّة المشروع
14	• العوائد المُتوقّعة من المشروع
15	المِخْوَْر الثّاني: دليل أوّلياء الأمور
17	• فكرة الدّليل وأهمّيّته
18	• أهداف الدّليل
19	• أسس ومُرتكّزات التّعامل مع الدّليل
21	المِخْوَْر الثّالث: الخصائص التّعليميّة للمُشاركين
24	• المرحلة الابتدائيّة
24	• طبيعة المرحلة
25	• المرحلة الإعداديّة

25	• طبيعة المرحلة
26	• المرحلة الثانوية
26	• طبيعة المرحلة
27	المِخْوََرُ الرَّابِعُ: المَوْضُوعَاتُ التَّدْرِيبِيَّةُ
29	• المَرْحَلَةُ الْإِبْتِدَائِيَّةُ
31	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ الْأُولَى: مَخَاطِرُ الْأَمْنِ السَّيْبِرَانِيِّ
41	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ الثَّانِيَّةُ: التَّنَمُّرُ عَبرَ الْإِنْتَرْنِتِ وَكَيْفِيَّةُ مُوَاجَهَتِهِ
49	• المَرْحَلَةُ الْإِعْدَادِيَّةُ
51	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ الثَّلَاثَةُ: التَّزْوِيرُ وَالْإِحْتِيَالُ عَبرَ الْإِنْتَرْنِتِ
59	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ الرَّابِعَةُ: هُجُومُ التَّنْصِيدِ الْإِحْتِيَالِيِّ
67	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ الْخَامِسَةُ: حُقُوقُ التَّأْلِيفِ وَالنَّشْرِ
73	• المَرْحَلَةُ الثَّانَوِيَّةُ
75	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ السَّادِسَةُ: بروتوكول IMAP4
81	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ السَّابِعَةُ: رِبُوتَاتُ الشَّبَكَةِ الْعَالَمِيَّةِ
89	◇ الحَقِيقَةُ التَّدْرِيبِيَّةُ الثَّامِنَةُ: سِيَاسَةُ أَمَانِ الْمَحْتَوَى
95	• الحَقِيقَةُ التَّدْرِيبِيَّةُ الْخَاصَّةُ بِأَوْلِيَاءِ الْأُمُورِ
95	◇ حِمَايَةُ الْأَجْهَازَةِ الْإِلِكْتُرُونِيَّةِ وَمُوَاجَهَةُ الْإِخْتِرَاقَاتِ الْأَمْنِيَّةِ

101	المحور الخامس: الألعاب التدريبية التفاعلية
104	• اللعبة الأولى: لعبة Cyber Block
105	• اللعبة الثانية: Cyber Quiz
106	• اللعبة الثالثة: سيبرونو Cyberno
107	• اللعبة الرابعة: سايبّر واي Cyber Way
108	• اللعبة الخامسة: بطاقات الأفكار التعليمية
109	المحور السادس: الدور المتوقع من أولياء الأمور في مشروع سايبّر إيكو
111	• الفرق بين الأنشطة الصفية واللاصفية
111	• توفير الوسائط الثقافية
112	• الدور المتوقع من أولياء الأمور
113	• تكامل دور أولياء الأمور مع دور المعلمين



تمهيد

يَشهد الإنترنت على مُستوى العالم انتشارًا وتطوُّرًا مُتسارعًا؛ بحيث بات جزءًا أصيلًا من حياة الدَّول والمجتمعات والأفراد، ووفقًا للتقارير والدَّراسات الدَّولية؛ فإنَّ التَّهديد الرِّقْمِيَّ يُعدُّ الأخطر على مستوى الأطفال واليافعين، وهو ما يُنطبق على دولة قطر، خاصَّةً أنَّ هذه الشَّرائح لديها خبرة بسيطة ومتواضعة في التَّعامل مع مَخاطر الإنترنت.

وانطلاقًا من سَعْيي الوكالة الوطنيَّة للأمن السيبرانيّ لتعزيز مستوى الأمان الرِّقْمِيَّ على مستوى كافَّة الشَّرائح الاجتماعيَّة، وعلى رأسها الأطفال واليافعون.



جاء مشروع الزيارات الميدانية للمدارس ليكون الأداة الفعلية والمنطلق التنفيذي الذي من خلاله سيتم تعزيز وعي الطلبة بمفاهيم الأمن السيبراني والسلامة الرقمية، من خلال التوجه بمحتوى تدريبي توعوي يستهدف الطلبة من الصف الأول الابتدائي و انتهاءً بالثاني عشر الثانوي، وكذلك الكادر التربوي والتدريسي وأولياء الأمور، ويتمحور المشروع حول تنظيم زيارات ميدانية للمدارس الحكومية والخاصة في الدولة، ليساهم في تعزيز مشروع المناهج السيبرانية بمحتوى تدريبي وتوعوي مبتكر خلال ورش العمل المختلفة أثناء برنامج الزيارات.

المَحَوَّر الأول
مشروع سايبر إيگو



أنت في رحاب
مدرسة الشفاء بمنت عبد الرحمن الانتصارية
حاضرة التميز والإبداع

1
2
3
4

مبادرة للتوعية بالأمن السيبراني
Cyberia

ومن هذا المنطلق دشنت
الهيئة العامة للغذاء والدواء
National Cyber Security Agency

أنت في رحاب
مدرسة الشفاء بمنت عبد الرحمن الانتصارية
إعدادت في مدرسة الشفاء بمنت عبد الرحمن الانتصارية

1
2
3
4

الهيئة العامة للغذاء والدواء
National Cyber Security Agency

مدرسة الشفاء بمنت عبد الرحمن الانتصارية
مناهج الأمن السيبراني للتطبيقية

Cyber Security Curriculum Education

الهيئة العامة للغذاء والدواء
National Cyber Security Agency



نظرة عامة على المشروع

الفكرة الأساسية لمشروع سايبر إيكو هي تعزيز وعي الطلّبة بمفاهيم الأمن السيبرانيّ والسّلامة الرّقميّة، من خلال تقديم محتوى تدريبيّ توعويّ للطلّبة في المدارس من مختلف المراحل التّعليميّة، وذلك من خلال أنشطة تفاعليّة تضمّن تفاعل وانسجام الطّلبة معها، وتبتعد فكرة المشروع تمامًا عن التّلقين أو المحتوى التّقليديّ، وبدلًا من ذلك تمّ الاعتماد على أساليب جديدة ومبتكرة، مثل التّدريب التّفاعليّ واعتماد أساليب تدريبيّة قائمة على الألعاب التّربّيّة والفيديوهات التّعليميّة والمسابقات.



دلالة اسم المشروع

«سَايْبَر إِيكُو» ينقسم اسم المشروع إلى شَقَّيْنِ: الأوَّل هو سايبِر، وهو يُعبِّر عن العَالَم الرِّقْمِيّ، والفضاء الإلكترونيّ الذي أصبح أهمَّ سِمَة من سمات العصر، والشَّق الثاني «إيكُو» وهو اختصار لكلمة Ecosystem، والتي تعني النِّظام البيئيّ، وبذلك يُصبح الاسم بالكامل سايبِر إيكُو يُشير لبناء بيئة سيبرانيّة مُحيطَة بالطَّلبة.

الفئات المُستهدَفة بالمشروع

- الطَّلبة في المدارس الحكوميّة والخاصّة وفي كلّ المراحل التَّعليميّة.
- المُعلِّمون والكوادر التَّربويّة.
- أولياء الأمور.

رؤية المشروع

تحويل السَّلامة الرِّقْمِيّة إلى مُمارَسة مُستدامة لدى الأطفال واليا فعي ن في دولة قطر.

رسالة المشروع

تعزيز وعي طلبة المدارس في دولة قطر بمفاهيم الأمن السيبرانيّ والسَّلامة الرِّقْمِيّة.

أهداف المشروع

- زيادة وعي الجمهور المُستهدف بمفاهيم الأمن السيبراني والسلامة الرقمية.
- تقديم المحتوى التدريبي والتوعوي للطلبة بأسلوب تفاعلي.
- تعزيز وتنمية المواهب الرقمية لدى الطلبة.
- تعزيز مستوى التواصل بين الكادر التدريسي وأولياء أمور الطلبة.
- تعزيز مستوى مؤشرات الأمن السيبراني والسلامة الرقمية في دولة قطر.

أهمية المشروع

- زيادة الاهتمام العالمي بفكرة توعية الطلبة من الأطفال والياfecين بهذا المجال الحيوي الاستراتيجي.
- حتمية توسيع نطاق التوعية بهذا المجال وتعريف الطلبة بمعنى الاستخدام المسؤول وأمن تكنولوجيا المعلومات والاتصالات.
- تدريب وتعليم الشباب القطري على التعامل بكفاءة واحترافية مع كل أشكال التكنولوجيا الرقمية لكي يكونوا نواة خبراء مُتخصصين في هذا المجال في المستقبل.
- ضرورة مواكبة التطور المستمر والسريع في أدوات التدريب والتأهيل خاصة في مجال الأمن السيبراني.





العوائد المَتَوَقَّعة من المشروع

- تعزيز المحتوى العلمي لمناهج الأمن السيبراني لدى طلبة المدارس بمحتوى تدريبي تفاعلي متنوع ومتميز.
- توفير حالة من التنافس الدائم بين الطلبة على الابتكار في المجال السيبراني، وتحفيزهم على تقديم أفكار مشروعات مبتكرة.
- خفض معدلات الظواهر السلبية المرتبطة باستخدام الإنترنت لدى الطلبة.
- دعم الخطط الوطنية للدولة لبناء ودعم المواهب السيبرانية من طلبة المدارس.
- ترسيخ واقع دولة قطر كدولة متميزة في مجال السلامة الرقمية وسلامة الطفل على الإنترنت.
- ترسيخ ثقافة السلامة الرقمية لدى مختلف شرائح المجتمع في دولة قطر، لا سيما لدى الأطفال والشباب.

المِخْوَر الثَّانِي
دليل أولياء الأمور

يُعَدُّ أولياء الأمور من المحاور المهمة في مشروع سايبير إيكو، خاصةً أنهم ومن خلال تعاملهم الدائم مع أبنائهم بإمكانهم الإسهام وبشكل مباشر في إنجاح المشروع وتحقيق أهدافه، لذلك جاء هذا الدليل ليكون بمثابة مُوجِّه عامٍّ لهم في كيفية التعامل والتعاون مع المشروع، ويوضح لهم كيفية التعامل مع أبنائهم وأهميته تواصلهم مع المعلمين لتحقيق أفضل نتائج مُمكنة من المشروع.

فكرة الدليل وأهميته

تُستمدُّ فكرة الدليل في جوهرها من أهمية دور الأهل في التأهيل الرقمي للطلبة؛ فهم ومن خلال طبيعة العلاقة الأسرية التي تجمعهم بأبنائهم يُعدُّون الأكثر قرباً منهم، وهو ما يُعزِّز من قدرتهم على تحفيز تعاون وتفاعل الطلبة مع المحتوى التدريبي المُقدَّم في سياق المشروع؛ فتعاون وتفاعل الطلبة مع المُدرِّبين يُعدُّ عاملاً حاسماً في إنجاح المشروع وتحقيق أهدافه. كما تتسع فكرة الدليل لتشمل ضرورة تزويد أولياء الأمور بمعلومات تفصيلية عن المشروع؛ فالدور التوجيهي والتشجيعي المُتوقَّع من أولياء الأمور مرهون بإدراكهم التام لماهية المشروع وأهميته وأهدافه، وإدراك الطبيعة العامة لمحتواه التدريبي، ومن هذا المنطلق، فإن الدليل يسعى لإطلاع أولياء الأمور على مختلف التفاصيل ذات الصلة بالمشروع في إطاره العام والخاص، وتوضيح المهام المُتوقَّعة منهم ومن الطلبة، وتقديم توجيهات عامة لهم حول كيفية التعامل والتعاون مع المشروع وكوادره.

وفيما يلي تبيان للنقاط التي تُوضِّح أهمية الدليل:

- يُعدُّ أداة رئيسة لتزويد أولياء الأمور بمعلومات تفصيلية حول المشروع وأهدافه وأهميته وطبيعة محتواه التدريبي والتوعوي.
- ضرورة تزويد أولياء الأمور بمعلومات تفصيلية حول الدور المُتوقَّع منهم في سياق تنفيذ المشروع.
- النجاح التام للمشروع يتطلَّب التعاون التام بين أولياء الأمور وبين مُعلِّمي الصف، والدليل يُعدُّ أداة رئيسة في توجيه وتنظيم هذا التعاون.
- ضرورة دمج أولياء الأمور في المشروع، على اعتبار أنهم الأقرب من أبنائهم والأقدر على التعامل التربوي معهم، والدليل يوضح كيفية إدارة وتنظيم دورهم في المشروع.
- من الضروري استمرار دور أولياء الأمور في الإرشاد والتوجيه الرقمي للطلبة بعد انتهاء المشروع، والدليل يُعدُّ مدخلاً لتوضيح دورهم العام في متابعة التوجيه الرقمي للطلبة.



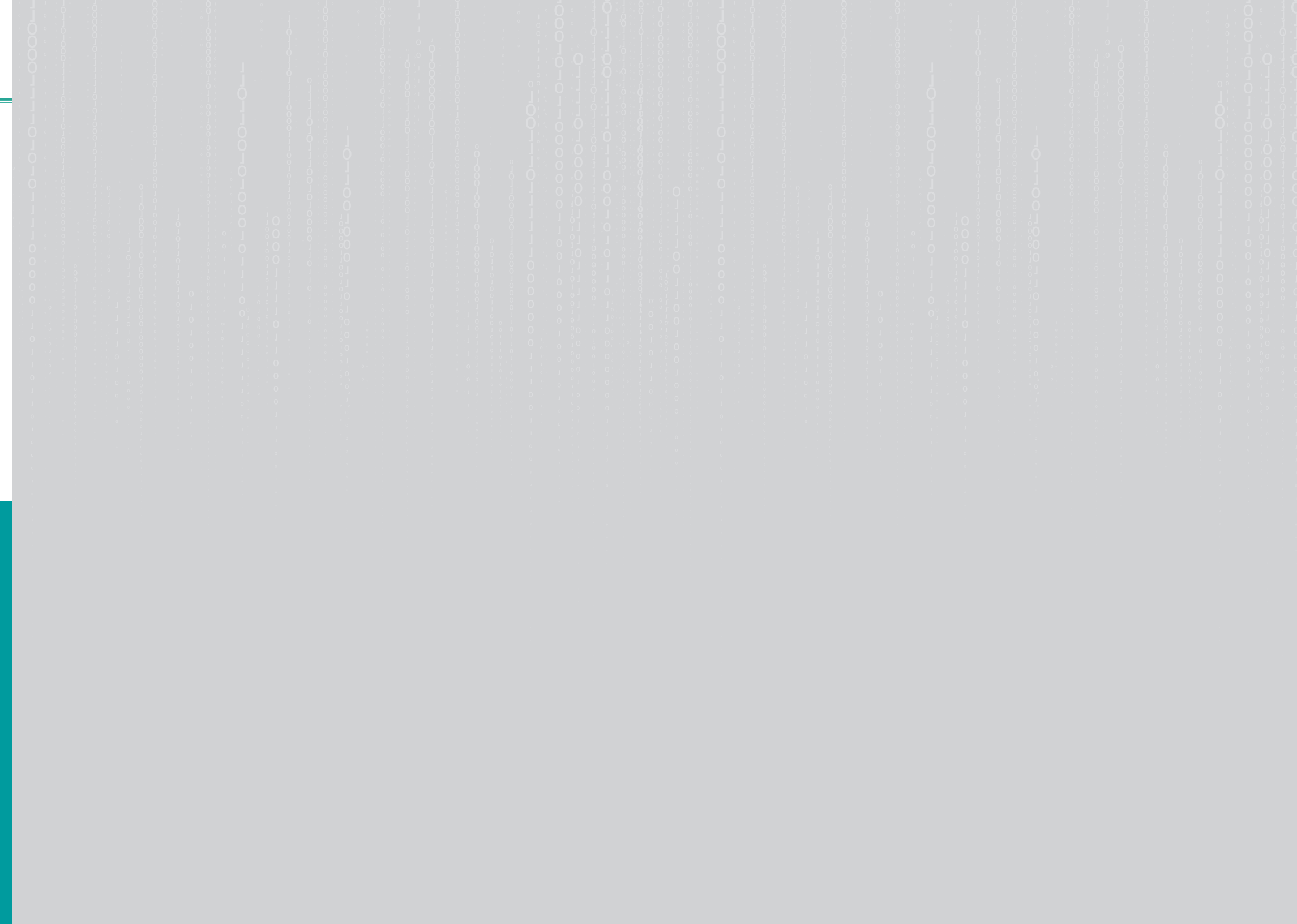
أهداف الدليل

- تزويد أولياء الأمور بمعلومات دقيقة وتفصيلية عن المشروع وأهدافه وأدواته.
- توضيح الدور المتوقع من أولياء الأمور في سياق المشروع، وتبيان كيفية الاضطلاع به؛ بما يعزز من فرص نجاحه وتحقيق أهدافه وبلوغ غايته ورؤيته.
- توضيح مُرتكزات التعاون بين أولياء الأمور وفريق تنفيذ المشروع، بما يضمن تحقيق أفضل النتائج الممكنة.
- ضمان تحقيق معدلات مرتفعة من التعاون والتفاعل بين الطلبة وفريق تنفيذ المشروع، من خلال تزويد أولياء الأمور بمعلومات وتوجيهات عامة حول هذا الأمر.

أُسُس ومُرتَكَزات التَّعامل مع الدَّليل

- الاطِّلاع على تفاصيل مشروع سايبر إيكو وأهدافه وأهمِّيته ورسالته ورؤيته، وإدراكها بدقَّة، والتي ذُكِرتْ تفصِيلاً في المِخْوَِر الأوَّل من هذا الدَّليل.
- الوَعْي التَّام بالمَهامِّ المُتَوَقَّعة من أوْلِياء الأُمُور، وإدراكها جيِّداً، والتَّهيَّئة للاطِّلاع بها، وهي مذكورة تفصِيلاً في سياق المِخْوَِر الخامس من هذا الدَّليل.
- الاطِّلاع العامَّ على المِخْوَِر العامَّة لِكُلِّ ورشة تدرِيبيَّة؛ بحيث يَطَّلِع أوْلِياء الأُمُور وبشكْلِ عامٍّ على السِّياق العامِّ للمُحتْوى التَّدرِيبيِّ المُقَدَّم في كُلِّ ورشة، وهي مذكورة تفصِيلاً في سياق المِخْوَِر الرَّابِع من هذا الدَّليل.





المَحْوَر الثالث
الخصائص التعليمية
للمُشارِكين

تعق الحركة

مدرسة عبد الله بن علي المسند الثانوية للبنين
ABDULLAH BIN ALI AL MANSUR SEC. SCHOOLS FOR BOYS

مركز مصادر التعلم

سياسة استشارة مصادر المعلومات بمركز مصادر التعلم

الهدف من سياسة استشارة مصادر المعلومات هو توفير المعلومات التي يحتاجها الطالب في دراسته وتعليمه، وذلك من خلال توفير مصادر المعلومات المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة، وذلك من خلال توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.

وتتضمن سياسة استشارة مصادر المعلومات ما يلي:

- 1- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 2- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 3- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 4- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 5- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 6- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 7- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 8- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 9- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.
- 10- توفير المصادر المختلفة، مثل الكتب، والمجلات، والصحف، والبرامج، والوسائط المتعددة، وغيرها من المصادر، وذلك بطريقة سهلة وبسيطة، وذلك من خلال توفير بيئة التعلم المناسبة.

مركز مصادر التعلم

معرض أبحاث الطلبة الداخلي ٢٠٢٢ - ٢٠٢٣
للمدرسة منطقة الجوار و سفيحة

مدرسة
عبد الله بن علي المسند الثانوية للبنين



الخصائص التعليمية نعني بها الاختلافات الخاصة التي تُميز كل مرحلة تعليمية، والتي ترتبط بالخبرات والسلوكيات الخاصة بكل مرحلة، وهو ما يستدعي استخدام أساليب تناسب كل مرحلة تعليمية من المراحل المُستهدفة بالمشروع، خاصة أن التعليم والتدريب في هذه المبادَرة قائم على التفاعل وعلى العديد من الأدوات التفاعلية، والتي تحتاج إلى أدوات مُعيّنة تُناسب تلك المرحلة، وفي هذا المِخْوَِر من الدليل؛ سيتم توضيح الخصائص التعليمية والمعرفية الخاصة بكل مرحلة من مَراحل التعليم.



المرحلة الابتدائية

طبيعة المرحلة:

تتراوح هذه المرحلة ما بين سن السادسة إلى الثانية عشرة، وتلك المرحلة هي الأهم في عمر الطفل؛ حيث يتم فيها تعليم الأطفال السلوكيات الجيدة ويتعرف فيها الأطفال على كل الأشياء الجديدة في محيطهم، سواء في المنزل ومع الأسرة، أو في المدرسة، أو حتى على الإنترنت.

يبدأ الطفل الدراسة في هذه المرحلة، وتبدأ أفكاره في التغير وفي تعلم الكثير من الأشياء، والاختلاط بالكثير من الأشخاص، والطفل في تلك المرحلة يتأثر بشكل سريع بكل ما يتعرض له، ويترسخ في ذهنه، وعلى الرغم من أن التعليم في هذه السن أسهل من السن الأكبر؛ إلا أنه يحتاج إلى الكثير من الهدوء والصبر؛ لأن الطفل في هذا العمر لا يلم بالكثير من المهارات، وبالتالي يحتاج إلى التعرف عليها والتدرب عليها دون ضغوط.



المرحلة الإعدادية

طبيعة المرحلة:

مرحلة المراهقة، أو يمكننا القول المرحلة الانتقالية ما بين الصغار في المرحلة الابتدائية، والشباب في المرحلة الثانوية، مرحلة يُظهر فيها الطالب العديد من التغيرات على مستوى الشكل والشخصية والحالة العقلية والعاطفية والاجتماعية، بالإضافة إلى التغيرات الهرمونية، وتتميز هذه المرحلة بالخصائص التالية:

- الطالب بدأ يُدرك العالم من حوله بشكلٍ واقعيٍّ أكثر.
- بدأ في استيعاب أن ما يفعله له آثار طويلة المدى.
- أصبحت العديد من الموضوعات لديه مُبهمة، ويحتاج إلى مُساعدة في استيعابها بطرق غير تقليدية.
- يُطوّر التفكير بطريقة ملموسة، ويمكنه استيعاب المفاهيم المُختصرة والرّموز.
- لديه نزعة أنانية، وقد يهمل الاهتمام بمشاعر الآخرين.



المرحلة الثانوية

طبيعة المرحلة:

في هذه المرحلة يقترب الطالب من النُمو التام والوصول إلى مرحلة الشباب، وهو ما ينتج عنه بعض التغيرات السلوكية، من أبرزها:

- الرغبة في التمرد والانصراف عن الدراسة.
- الاعتماد على الحيل الدفاعية من أجل التهرب من المهام خاصة الدراسية.
- إبداء حالة عدم الاهتمام والتجاهل.
- الانفعالات الحادة والتأثر الشديد وسرعة الغضب أحياناً.

وفي هذه المرحلة يزداد شغف الطلبة بالحاسوب والإنترنت، وبالتالي لديهم معرفة عميقة بما يفعلونه، لذلك لا بُد من الاستعداد جيداً للتعامل المعرفي معهم.

المَحَوْر الرَّابِع

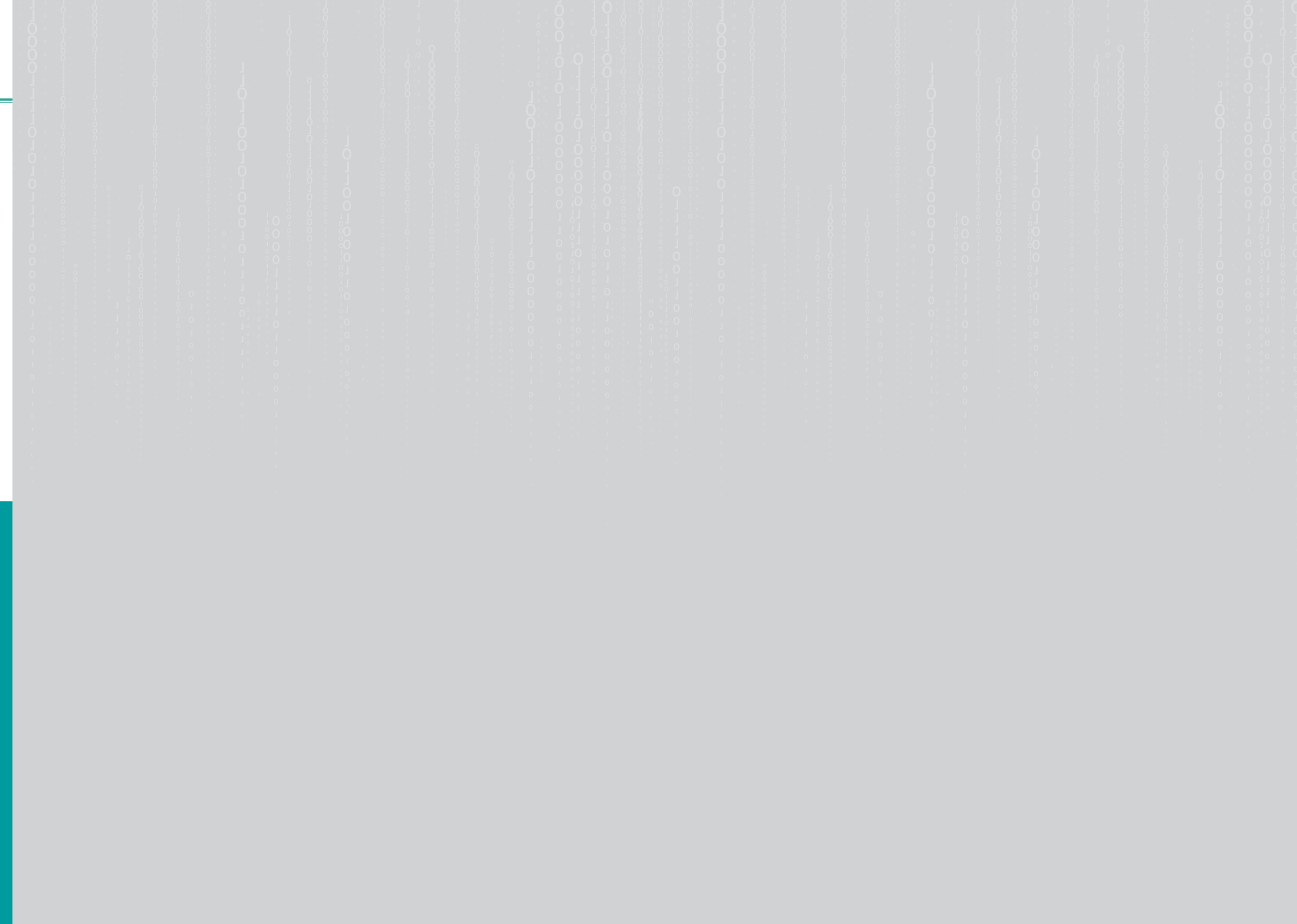
المَوْضُوعَاتُ التَّدْرِيبِيَّةُ



في هذا المَحْوَِر من الدَّلِيل سَيُتَمَّ تقديم عَرَضٍ تلخيصيٍّ للمَوْضوعات التَّدْرِيبيَّة التي سَيُتَمَّ التَّوَجُّه بها للمُسْتَهِدِّين بمَشْرُوع الزِّيَارَات المِيدَانِيَّة «سَايِر إِيكُو»، وسَيُتَمَّ تقسيم المَوْضوعات التَّدْرِيبيَّة وَفَقًّا للمراحل التَّعليميَّة. وانطلاقًا من أَهمِّيَّة اِطِّلاع أَوْلِيَاء الأُمُور على المَحْتَوَى التَّدْرِيبيِّ الذي سَيُتَمَّ تقديمه للمُسْتَهِدِّين بالمَشْرُوع، سوف يُقَدِّم هذا المَحْوَِر معلومات مُختصرة عن المَوْضوعات التَّدْرِيبيَّة، وأهمَّ المعلومات التي سَيُتَمَّ تقديمها لهم من قِبَل فريق المَشْرُوع.

المَرْحَلَةُ الإِبْتِدَائِيَّة

في هذه المَرْحَلَة سَيُتَمَّ تقديم التَّدْرِيِب الرِّقْمِيِّ من خلال مَحْوَِرَيْن اثْنَيْن؛ هما مَخاطر الأَمْن السَّيْبِرَانِيّ والتَّنَمُّر عبر الإنترنت وكَيْفِيَّة مَواجهته، وفيما يلي تبيان لأهمَّ المعلومات التي سَيُتَمَّ تقديمها في هَذَيْن المَحْوَِرَيْن.



الحَقِيبَةُ التَّدْرِيبِيَّةُ الْأُولَى



مَخَاطِر الْأَمْنِ السَّيْبِرَانِيِّ

الفصل الأول: مفهوم الأمن السيبراني والسلامة الرقمية
الفصل الثاني: المخاطر المرتبطة بالأمن السيبراني
الفصل الثالث: كيف أحمي نفسي من التهديدات الرقمية؟

القراءة هي
متعة التجول في
عقول الآخرين

مدرسة عبدالرحمن عيال المسند الإعدادية
تحيات السيدة الضيوف من
الوكالة الوطنية للأمن
السبراني



هناك دائماً العديد من المخاطر التي تترتب بمُستخدمي الإنترنت، تلك المخاطر قد تتسبب في مُشكلات كبيرة في الأصول أو البيانات الخاصة بالمُستخدمين، وغالباً ما تكون تلك المخاطر مقصودة ومُوجّهة بفرض سرقة المال أو المعلومات والبيانات.

الفصل الأول: مفهوم الأمن السيبراني والسلامة الرقمية الأمن السيبراني:

الأمن السيبراني هو كُل الممارسات التي يتم من خلالها حماية أجهزة الحاسوب والشبكات وتطبيقات البرامج والأنظمة المهمة والبيانات من التهديدات الرقمية المحتملة، وتقع مهمة الحماية هذه على عاتق المؤسسات خاصة تلك التي تمتلك بيانات العملاء، والتي لا بُد أن تعتمد على تدابير وأدوات تساعد في ضمان الأمن السيبراني، وحماية البيانات الحساسة من كُل مُحاولات الوصول غير المصرح بها.

أما السلامة الرقمية، فهي:

كُل الأنشطة والإجراءات التي تستهدف حماية البيانات الشخصية والأصول الرقمية الخاصة بك على الإنترنت، والسلامة الرقمية تُعد جزءاً من الأمن السيبراني، فالأمن السيبراني مفهوم أوسع وأشمل، فهو يشغل مساحة أوسع في الحماية الرقمية، يشمل حماية الشبكات وأنظمة التشغيل، والبيانات المُخزنة بداخلها من التهدي أو التخريب أو الوصول غير المصرح به.



الفصل الثاني: المخاطر المرتبطة بالأمن السيبراني

أصبح الإنترنت جزءًا لا يتجزأ من الحياة اليومية لأغلب سُكَّانِ العالم، ويمكن الاستفادة من الإنترنت في الكثير من الأمور بشكل يومي، ولكن مع زيادة الاعتماد على الإنترنت ظهرت لنا العديد من الجرائم الإلكترونية، والتي تحدث في الفضاء الرقمي، وعلى الرغم من ذلك تمتد مخاطرها إلى العالم الواقعي.

مخاطر الإنترنت

- **التتبع عبر الإنترنت:** وهو التعرض للسخرية على الإنترنت؛ سواء في الأحاديث المتبادلة على مواقع التواصل الاجتماعي أو في التعليقات على المنشورات والصور، أو من خلال الألعاب.
- **نشر المعلومات الخاصة:** يقع الكثير من الأطفال في هذه المشكلة نظرًا لعدم إدراكهم الحدود التي لا بُدَّ التقيّد بها أثناء النشر على الإنترنت، فهناك العديد من المعلومات الشخصية والبيانات التي يجب عدم مشاركتها مع الآخرين مثل عنوان المنزل، اسم المدرسة، منطقة الإقامة، وخاصة العامة منها.

- **التصيد الاحتيالي:** وهو نوع من أنواع الاختراق يعتمد على خداع المستخدمين من أجل فتح رابط ما أو مرفقات في البريد الإلكتروني، ومن ثم يحدث الاختراق، والذي يمكن من خلاله مراقبة المستخدمين، أو الوصول إلى الكثير من البيانات والمعلومات التي قد تتسبب في خطر حقيقي على حياة المستخدم وكل المحيطين به.
- **عمليات التصيب:** والتي تشمل الرسائل المخادعة التي يمكن أن تصل عبر الحاسوب أو الهاتف الذكي أو الجهاز اللوحي للعبة مجانية، أو هدية هاتف جديد بمقابل بسيط، وعليه يرسل المستخدم أرقام بطاقة الائتمان، وبدلاً من تلقي هدية يسحب الرصيد الخاص به دون عوذة.
- **البرمجيات الضارة:** يمكن أن يتم تحميل تلك البرمجيات دون رغبة المستخدم أو إذنه، وتتسبب تلك البرمجيات في أضرار كبيرة على أجهزة الحاسوب أو الهواتف أو أي جهاز مرتبط بالإنترنت؛ مثل سرقة البيانات، أو التهديد من أجل الحصول على فدية، أو غيره من المشكلات التي قد تسببها تلك البرمجيات.

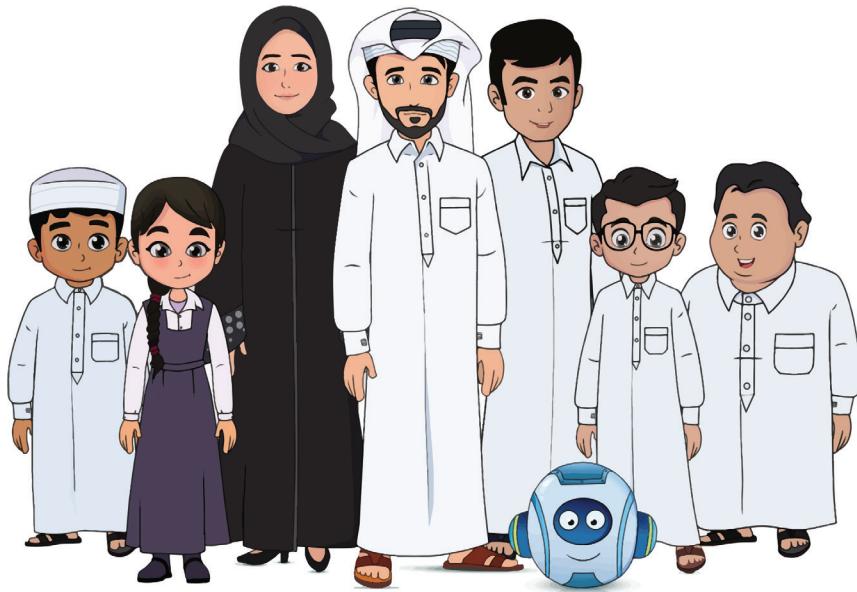
مَخاطر سرقة البيانات الشخصية

سرقة البيانات أو المعلومات هي النّقل غير القانوني للمعلومات الشخصية أو السّريّة أو المعلومات الماليّة.

من أهمّ البيانات التي يسعى المُخترِقون إلى سرقتها:

- معلومات الحسابات البنكيّة.
- كلمات المرور.
- أرقام جواز السّفَر.
- أرقام الهوية الوطنية (الرقم الشخصي).
- أرقام رُخص القيادة.
- أرقام الضّمان الاجتماعيّ.
- السّجلات الطّبيّة.
- المعلومات الخاصّة بالاشتراكات.

وغالبًا ما يتمّ بيع المعلومات التي تمّ سرقتها، أو يمكن استغلالها من أجل الحُصول على أرباحٍ ماديّةٍ من وراء هذه السّرقَة، خاصّةً الحسابات البنكيّة.



أما عن طريقة سرقة البيانات فغالبًا ما تحدث بإحدى الطُّرُق الآتية:

- **الهندسة الاجتماعية**، والشكل الأكثر شيوعًا فيها هو التصيد الاحتيالي، ويتم فيه التَّنكر في صورة هيئة أو جهة مَوْثوقة من أجل خداع الضحية ودفعه لفتح رسالة ما.
- **كلمات المرور الضعيفة والتي يسهل تخمينها أو توقعها.**
- **الثغرات الأمنية**، وقد تتسبب فيها التطبيقات أو البرمجيات غير الآمنة أو ذات التصميم السيئ، والتي يستغلها لُصوص البيانات من أجل الدُّخول وسرقة بيانات المُستخدمين.

- **الأخطاء البشرية**، فيمكن أن تكون السرقة حدثت بسبب تسريب من صاحب البيانات نفسه، والذي قام بمُشاركة البيانات الخاصة به دون أن يدرك أنَّ هناك خطورة في الأمر وربما تكون تلك البيانات وصلت عن طريق الخطأ إلى جهة غير صحيحة وهو ما أدَّى إلى تسريبها.
- **المعلومات المُتاحة للجمهور**، والتي غالبًا ما توجد في منشورات منصات التواصل الاجتماعي المُختلفة والتي يشارك فيها الناس بحريَّة تامَّة العديد من البيانات والمعلومات الشخصية التي يمكن أن تكشف الكثير عنهم، حتَّى دون أن يدركوا ذلك.

مخاطر سرقة البيانات

- يمكن أن تتسبب سرقة البيانات في تسريب بيانات العملاء الخاصة لدى الشركات والمؤسسات.
- يمكن أن يطلب المهاجمون فدية مالية كبيرة مقابل استرجاع البيانات.
- الإضرار بالسمعة وفقدان الثقة بالإضافة إلى المسؤولية القانونية.
- التكاليف الخاصة باسترجاع البيانات أو إعادة تأمين الخوادم وقواعد البيانات.
- إهدار الوقت بسبب تعطل الأنظمة أثناء وبعد عمليات الهجوم.
- التكاليف المالية بسبب سرقة البيانات المصروفة.
- الأضرار النفسية التي قد تنتج عن سرقة البيانات والمعلومات.

مخاطر التتمر عبر الإنترنت

التتمر عبر الإنترنت هو استغلال الإنترنت وكل التقنيات التكنولوجية الحديثة من أجل إيذاء شخص أو أشخاص آخرين بطريقة متعمدة ومتكررة، والتتمر هو سلوك عدواني سلبي وغير مرغوب فيه، ولكن هذه المرة يتم عبر الفضاء الإلكتروني من خلال الرسائل، أو التعليقات على منصات التواصل الاجتماعي أو مواقع الإنترنت، والهدف الأساسي منه هو إيذاء الضحية والإساءة إليها؛ سواء بشكل مادي أو معنوي أو اجتماعي أو نفسي.



وللتَّثْمَرِ عبر الإنترنت العديد من الأشكال؛ أهمّها:

- **المُضايقة**، من خلال إرسال رسائل مُسيئة أو غير لائقة، أو كتابة تعليقاتٍ سلبيةٍ مُهينةٍ على كُلِّ ما يشاركه الضَّحية على مواقع التَّواصل الاجتماعي.
- **تشويه السمعة**، وهي ببساطة نُشر معلوماتٍ غير صحيحةٍ أو شائعاتٍ غير حقيقيةٍ حول أشخاصٍ آخرين بهدف السُّخرية أو تشويه السمعة.
- **سرقة الهوية**، ويحدث حين يخترق شخصٌ حساب شخصٍ آخر ويبدأ في استخدام حساباته وكتابه ومُشاركة أشياء وموادَّ مُحرجة ومُسيئة.
- **المُطاردة الإلكترونية**، ومعناها إرسال رسائل إلكترونية بِشكْلِ مُتكرِّرٍ بهدف التهديد أو المُضايقة أو التَّخويف، وتتنسَّب في شُعُور الضَّحية بالخوف والقلق.
- **النُّبذ والاستبعاد الإلكتروني**، ويحدث هذا حين يتمَّ تعمُّد ترك شخصٍ ما خارج المجموعة أو استبعاده من لُعبةٍ ما، ويُعدُّ هذا شكلاً من أشكال التَّثْمَرِ الاجتماعي.
- **القرصنة الإلكترونية**، وهي عبارة عن الاعتماد على برمجيات ضارة أو سرقة كلمات المرور من أجل التَّحكُّم في حسابات أو أجهزة الضَّحية.

- **التَّثْمَرِ من خلال الصُّور**، هو نُشر صُور غير لائقةٍ للضَّحية، أو تصوير الضَّحية بدون علمه ونُشر الصُّور على منصات التَّواصل الاجتماعي.
- **التَّجسس**، وذلك من خلال استخدام تطبيقاتٍ مُعيّنة تحاول خَرْق حُصُونِ الآخرين من خلال خداعهم، وبعدها يقوم المُتتَمِر بِنشر تلك المعلومات الخاصة وإرسالها للآخرين للإضرار بالضَّحية.

أما عن مَخاطر التَّثْمَرِ فتشمل:

- شُعُور الضَّحية بالوَحدة والعُزلة والرَّغبة في الابتعاد كلياً عن التَّجمُّعات والبقاء مع الآخرين.
- الشُّعُور بالخزي والعار، وبالتالي الشُّعُور بالقلق والضيق والحرَج.
- فُقدان الثقة بالنفس وكذلك الثقة بالآخرين.
- تدني احترام الذات والشُّعُور بالنقص وانعدام القيمة والأهميّة.
- بعض المُشكلات الضَّحية للضحايا؛ خاصّةً تلك التي تتعلَّق بالطَّعام والنُّوم.
- التَّأخُّر في التَّحصيل الدَّرَاسي أو الالتزام في العمل.
- الشُّعُور بالخوف الدائم وانعدام الأمان.

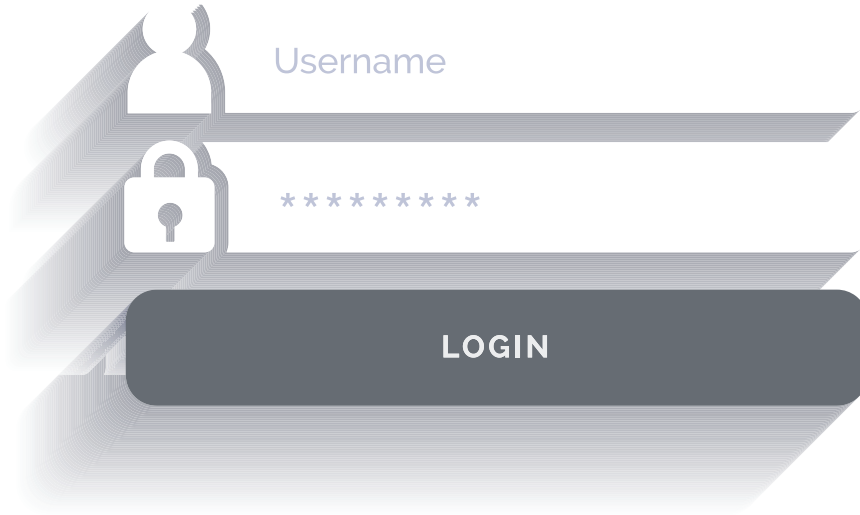
الفصل الثالث: كيف أحمي نفسي من التهديدات الرقمية؟

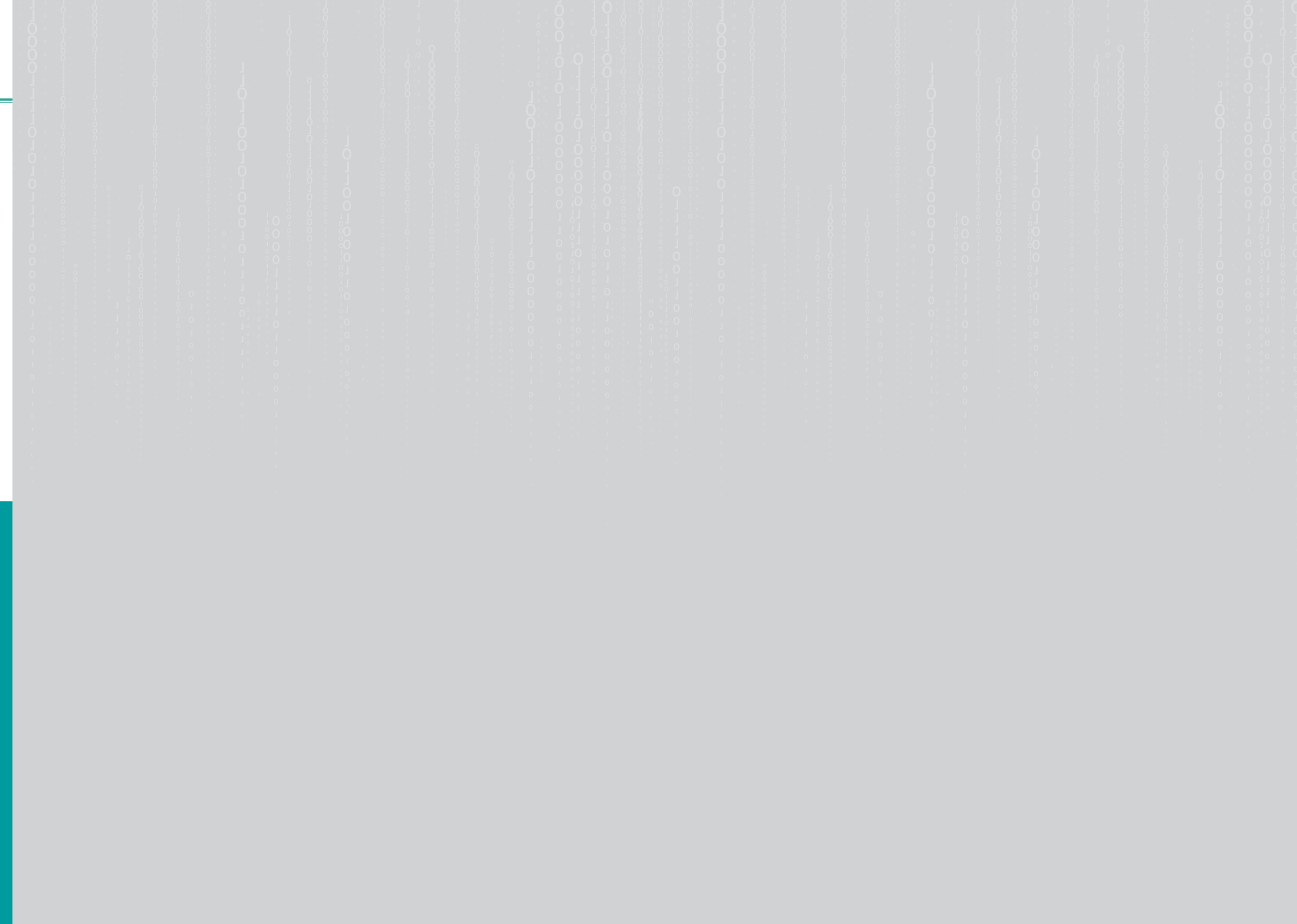
استخدام كلمات المرور القوية لحماية البيانات

يساعد استخدام كلمة مرور قوية على الحفاظ على أمان المعلومات الشخصية، وكذلك رسائل البريد الإلكتروني، بالإضافة إلى حماية الملفات والبيانات الأخرى.

كيفية كتابة كلمة سر قوية

- لا بد أن تكون مكونة من أكثر من 10 - 12 حرفًا ورقمًا.
- يُفضل استخدام الرموز والأحرف والأرقام.
- من المهم استخدام الحروف الكبيرة والصغيرة.
- تجنب استخدام تاريخ الميلاد، أو التواريخ المميزة.
- تجنب استخدام كلمة Password.
- تجنب ربط الحسابات كلها بكلمة مرور واحدة.
- عدم استخدام بيانات شخصية أو كلمات شائعة.
- استخدام كلمة مرور يمكن تذكرها ولا يمكن للآخرين تخمينها.
- استخدام خاصية التحقق بخطوتين، أو إضافة بريد إلكتروني مخصص لاسترداد كلمة المرور.



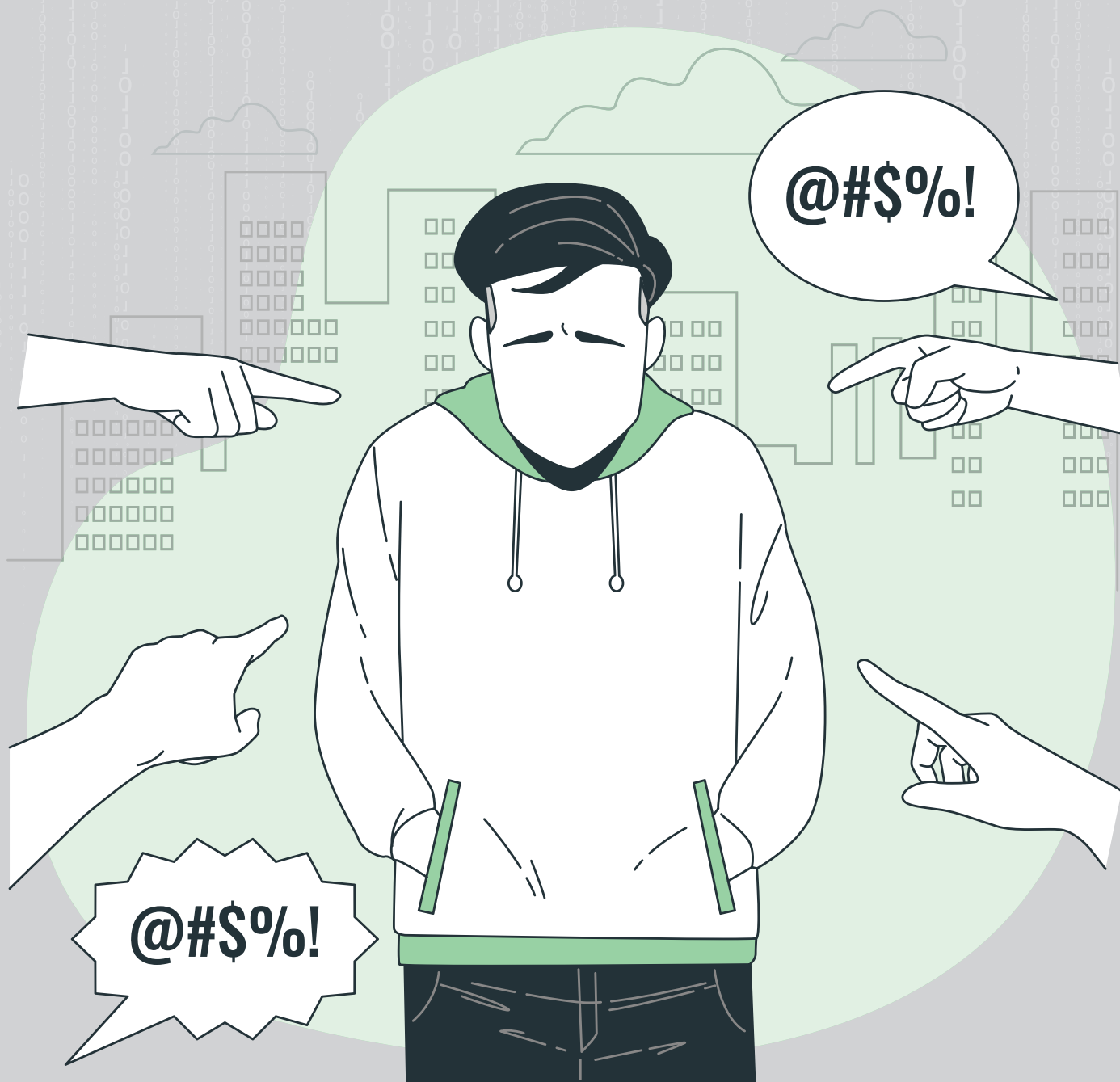


الحَقِيبَةُ التَّدْرِيبِيَّةُ الثَّانِيَّةُ



التَّنَمُّرُ عِبْرَ الْإِنْتَرْنِتِ وَكَيْفِيَّةُ مُوَاجَهَتِهِ

الفصل الأول: مفهوم التَّنَمُّرِ عِبْرَ الْإِنْتَرْنِتِ
الفصل الثاني: كَيْفِيَّةُ مُوَاجَهَةِ مَخَاطِرِ التَّنَمُّرِ عِبْرَ الْإِنْتَرْنِتِ



أصبح التَّثْمَرُ عَبرَ الإنترنت أحد أبرز المخاطر الموجودة على شبكة الإنترنت، وخاصةً تجاه الأطفال، ولذلك لا بُدَّ من توعية الأطفال بشأن التَّثْمَرِ عَبرَ الإنترنت، وتعليمهم تَبْذُ هذا السُّلُوكَ تمامًا مُنْذُ الصَّغَرِ.

الفصل الأول: مفهوم التَّثْمَرِ عَبرَ الإنترنت

يُعرِّض أغلب مُستخدمي الإنترنت للتَّثْمَرِ الإلكتروني، والذي غالبًا ما يظهر في الأحاديث المُتبادلة عَبرَ الإنترنت، أو في التعليقات على المنشورات على مواقع التواصل الاجتماعي، ولكن الأطفال غالبًا ما يكونون الأكثر عُرضة لهذا النوع من السُّلُوكِ، وللأسف يتأثرون بِشَكْلِ كبيرٍ بهذا المَحْتَوَى، وقد يصل الأمر ببعضهم إلى الإصابة بالاكْتِئاب.

ما المقصود بالتَّثْمَرِ عَبرَ الإنترنت؟

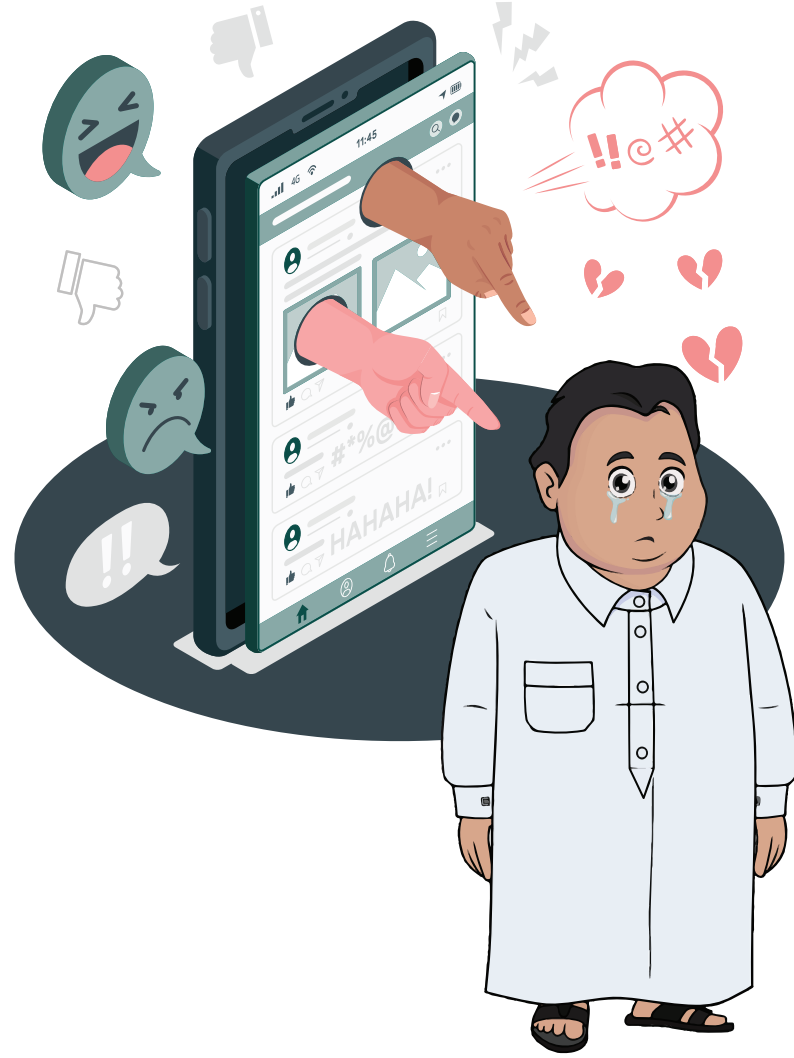
التَّثْمَرُ عَبرَ الإنترنت هو استخدام الإنترنت أو تقنيات التواصل من أجل إيذاء أشخاص بعينهم أو إضرارهم بطريقة مُتعمَّدة ومُتكرِّرة وعدائية، والتَّثْمَرُ بِشَكْلِ عامٍّ هو سُلُوكٌ عُدْوانِيٌّ سَلْبِيٌّ وغير مرغوب فيه، ولكن هذه المرَّة يتم من خلال الفضاء الإلكتروني والأدوات التكنولوجية الحديثة، من خلال الرسائل أو التعليقات على منصات التواصل الاجتماعي أو مواقع الإنترنت، والهدف منه هو الإضرار بالصِّحَايا والإساءة إليهم.



ما هي مظاهر وأشكال التتُّم عبر الإنترنت؟

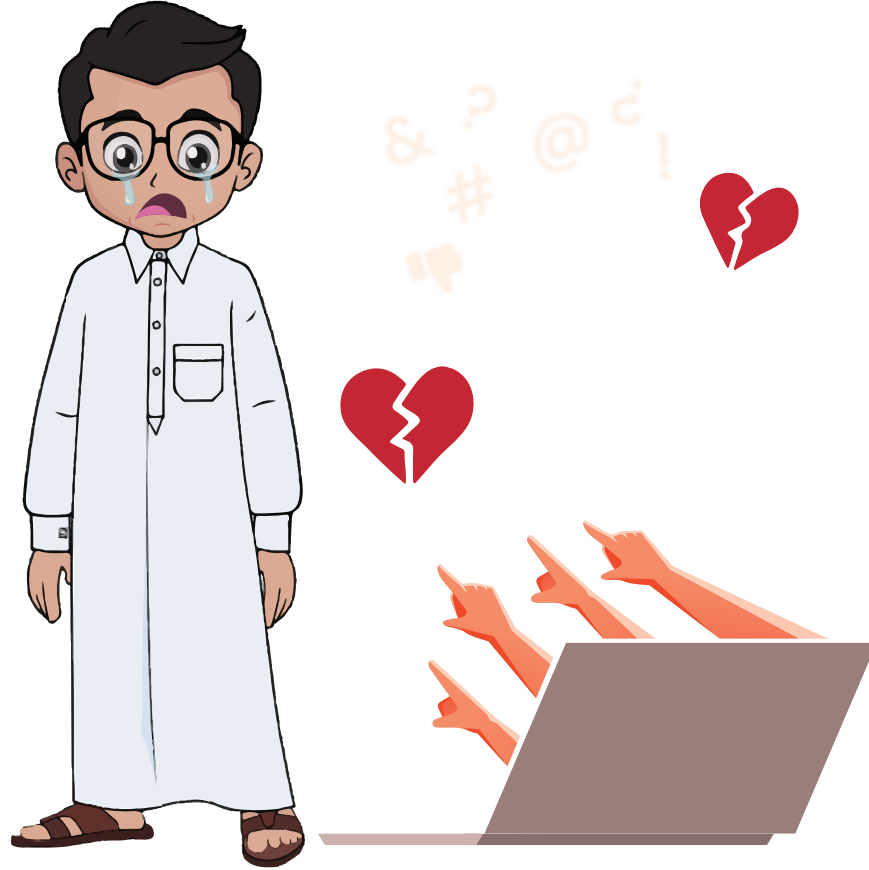
- **المُضايقات:** وذلك من خلال العمل على مُضايقة الضَّحية من خلال إرسال رسائل مُزعجة أو مُسيئة، أو التعليق بشكلٍ مُسيء على منشورات الضَّحية على وسائل التواصل الاجتماعي.
- **التتُّم من خلال الصور:** يحدث هذا الشُّكل من التتُّم من خلال نشر صور الضَّحية بدون موافقته على منصات التواصل الاجتماعي، أو نشر صور غير لائقة.
- **التجسس:** من خلال برمجيات خاصة بالتجسس، والهدف منها معرفة تفاصيل عن الحياة الخاصة بالضَّحية، واستخدامها لابتزازه أو إزعاجه.
- **الإضرار بالسُّمعة:** من خلال نشر شائعات أو معلومات غير صحيحة؛ بهدف التتُّم على الضَّحية والإساءة إليه.

- **المُطاردة:** وتسمى بالمُطاردة الإلكترونية، ويحدث هذا النوع من التتُّم من خلال إرسال رسائل تهديد أو إزعاج للضَّحية بشكلٍ مُستمر، ومن خلال عدّة منصات، كالبريد الإلكتروني أو منصات التواصل الاجتماعي.
- **سرقة الهوية:** يحدث هذا النوع من التتُّم من خلال إمّا خرق أحد الحسابات الشخصية للضَّحية والنشر باسمه، أو من خلال إنشاء صفحات ومواقع جديدة والادّعاء بأنها تعود للضَّحية، وذلك بهدف الإساءة إليه.
- **القرصنة:** وذلك من خلال استخدام برمجيات خبيثة لسرقة المعلومات الشخصية وكلمات المرور.
- **النُّبذ:** من خلال استبعاد شخص ما عن مجموعة أو لُعبة إلكترونية؛ وذلك بهدف مُضايقته.



الآثار الناجمة عن التَّمتُّر عَبرَ الإنترنت

- حين يحدث تَمَتُّر إلكتروني يشعر الضحية بأنه عُرضة للتَّمتُّر في أي وقت وفي أي مكان، فقد تعرَّض للتَّمتُّر وهو داخل منزله، وهو ما يُؤثر عليه على عدَّة مستويات:
- **عقليًا:** فيبدأ بالشُّعور بالضيق والحرج وحتى الشُّعور بالفُصْب.
 - **عاطفيًا:** يشعر بالخجل وفُقدان الاهتمام بالأشياء التي يُحبُّها.
 - **جسديًا:** لأن المُشكِلات النفسية تُؤثر عليه، وخاصَّةً على النَّوم وتناول الطعام، وبالتالي قد يُصاب بالآرق، آلام المَعِدَّة، الشره، أو فُقدان الشهية، وبالطبع الصَّدَاع.



مَخَاطِر التَّثَمَّرِ عِبْرَ الْإِنْتَرْنِت

- الشُّعُورُ بِالوَحْدَةِ وَالْعُزْلَةِ وَالرَّغْبَةُ فِي قِضَاءِ أَوقَاتٍ طَوِيلَةٍ بَعِيدًا عَنِ الْآخَرِينَ أَوْ الْمُنَاسَبَاتِ الْاجْتِمَاعِيَّةِ.
- الشُّعُورُ بِالْإِرْهَاقِ وَالْقَلَقِ وَالضُّيْقِ، بِالإِضَافَةِ إِلَى الشُّعُورِ بِالْحَرَجِ الشَّدِيدِ وَالْخِزْيِ خَاصَّةً فِي حَالَةِ تَشْوِيهِ السَّمْعَةِ وَنَشْرِ الشَّائِعَاتِ.
- انْعِدَامُ الثِّقَةِ بِالنَّفْسِ وَبِالْآخَرِينَ، وَالشُّعُورُ بِالنَّقْصِ وَانْعِدَامِ الْقِيَمَةِ وَالْأَهَمِّيَّةِ.
- مَعَانَاةُ الْكَثِيرِ مِنَ الْمَشْكِلاتِ الصَّحِيَّةِ وَالَّتِي تَظْهَرُ بِوُضُوحٍ عَلَى مَظْهَرِ الصَّحَايَا؛ لِأَنَّهَا تَرْتَبِطُ بِالطَّعَامِ وَالنَّوْمِ.
- الشُّعُورُ بِالْقَضْبِ الشَّدِيدِ وَالْإِكْتِنَابِ.
- التَّأَخُّرُ فِي التَّحْصِيلِ الدِّرَاسِيِّ وَفُقْدَانِ الْعَمَلِ.
- الشُّعُورُ بِالْخَوْفِ وَعَدَمِ الْأَمَانِ.

الفصل الثاني: كيفية مواجهة مخاطر التَّمتُّر عبر الإنترنت

كيف أحمي نفسي من التَّمتُّر عبر الإنترنت؟

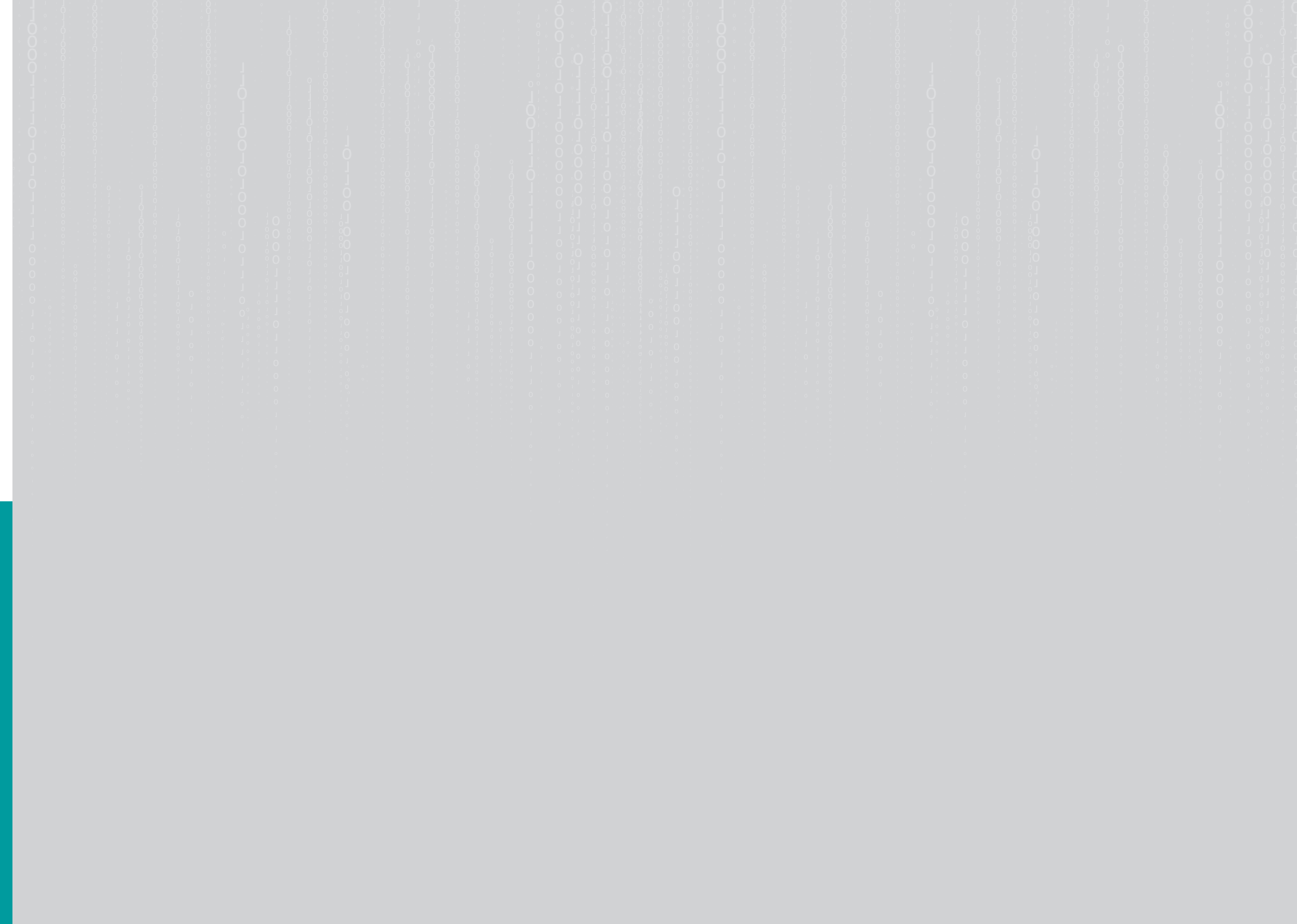
- تعليم الأطفال وتدريبهم على التَّعامل مع المُتَمَتِّرين، وتشجيعهم على الإفصاح عمَّا يحدث معهم للوالدين أو المُعلِّمين؛ لاتخاذ الإجراءات اللازمة.
- تعلُّم آداب الإنترنت قبل استخدامه.
- التَّعرُّف على القوانين وقواعد وسياسات المواقع، وبالتَّحديد مِنصات التَّواصل الاجتماعيِّ، خاصَّةً فيما يتعلَّق بالتَّمتُّر عبر الإنترنت ومُلاحقة المُتَمَتِّرين.
- التَّحقُّق على الصُّور والمعلومات الشَّخصية، خاصَّةً تلك التي يتمُّ تداولها عبر مواقع التَّواصل الاجتماعيِّ.
- الإصرار على اتِّخاذ الإجراءات القانونيَّة ضدَّ المُتَمَتِّرين وعدم التَّنازل أو إظهار الضَّعف أو الخوف منهم.
- تجاهل التَّعليقات المُسيئة والرسائل وعدم الردِّ عليها.

- حَظَر المُتَمَتِّرين فورًا وتجنُّب مُواجهتهم أو تهديدهم.
- استخدام كلمات مرورٍ يصعب توقُّعها أو اختراقها لحماية الحِسَابات مِن الاختراق.
- الحفاظ على سرِّيَّة بيانات الدُّخول وتجنُّب استخدام شبكات الإنترنت العامَّة، أو تسجيل الدُّخول أمام أيِّ شخصٍ.
- التَّأكُّد من تسجيل الخُروج في حالة استخدام جهاز غير جهازك، أو في حالة مُشاركة جهازك مع أشخاص آخرين.
- عدم الثِّقة بالقرَّباء وعدم إعطاء الآخرين أيِّ معلومات خاصَّة عنك، حتى وإن كنت تشعر أنَّهم محلَّ ثِقَةٍ وأمانٍ.



المرحلة الإعدادية

في هذه المرحلة سيتم تقديم التدريب الرقمي من خلال ثلاثة محاور، هي التزوير والاحتياز عبر الإنترنت، والتصيد الإلكتروني، وحقوق التأليف والنشر، وفيما يلي تبيان لأهم المعلومات التي سيتم تقديمها في هذه المحاور.



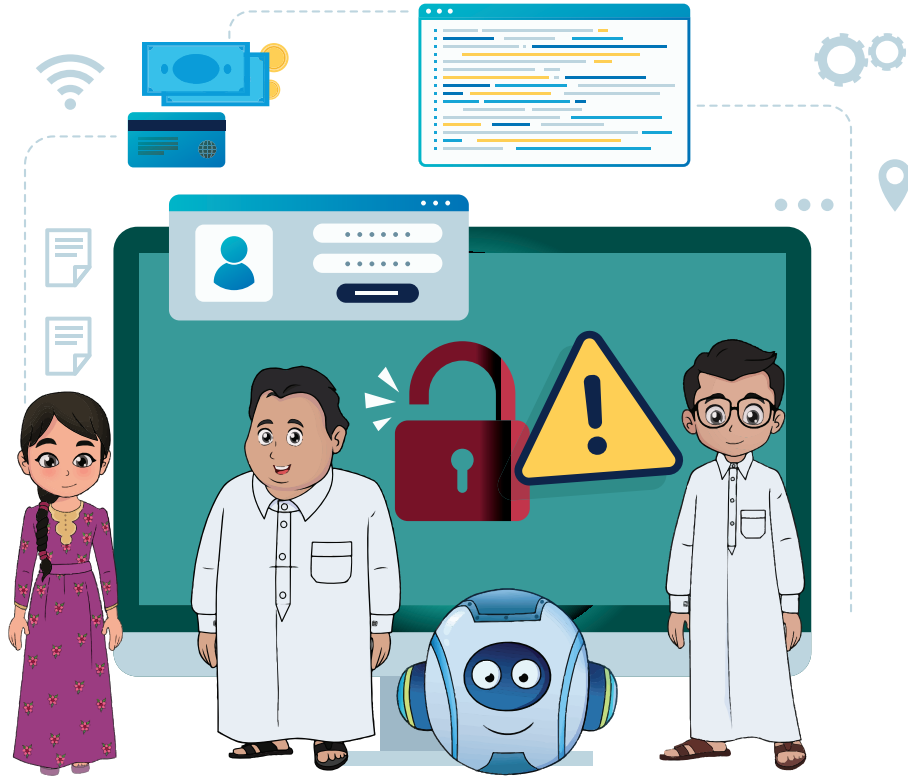
الحَقِيقَةُ التَّدرِيبِيَّةُ الثَّالِثَةُ



التَّزْوِيرُ وَالْاِحْتِيَالُ عِبْرَ الْإِنْتَرْنِتِ

الفصل الأول: مفهوم التزوير والاحتيال عبر الإنترنت وأنواعه
الفصل الثاني: كيفية تنفيذ عمليات الاحتيال عبر الإنترنت
الفصل الثالث: كيفية التصرف في حال التعرض للاحتيال عبر الإنترنت





الفصل الأول: مفهوم التزوير والاحتيال عبر الإنترنت وأنواعه

ثورة الإنترنت والنمو الكبير في التكنولوجيا سهلت الكثير من الأمور، ومن ضمنها المعاملات المالية والتجارية من خلال الوسائط التكنولوجية، وبالطبع معها تطورت وسائل الاحتيال عبر الإنترنت لتصبح تهديداً حقيقياً لأغلب مستخدميها، وهو ما يجعلنا كل يوم نتعرف على سبل وطرق ووسائل جديدة تم استخدامها في الاحتيال على الضحايا.

مفهوم الاحتيال عبر الإنترنت

الاحتيال عبر الإنترنت هو شكل من أشكال النصب، والهدف منه هو الاستيلاء على المعلومات والأموال أو الممتلكات بطرق غير مشروعة، ويتم باستخدام الإنترنت والبرمجيات التي تعمل من خلاله، وغالباً ما يؤدي إلى خسائر كبيرة، قد تصل إلى ملايين الدولارات سنوياً، بالإضافة إلى الخسائر المعنوية بالطبع.

أنواع وأشكال الاحتيال عبر الإنترنت

يمكن تنفيذ الاحتيال عبر الإنترنت عن طريق إحدى الأدوات الآتية:

- **البريد الإلكتروني:** وذلك حين تصلك رسالة بريد إلكتروني مغرية، بأنك قد فُزت في مُسابقةٍ ما أو لديك هاتف هدية أو عُطلة مجانية، كل ما عليك هو الضغط على الرابط، فور دُخولك يُطلب منك بعض البيانات الشخصية والمالية، أو يُطلب منك تحويل مبلغ بسيط للحصول على الجائزة، وبالطبع فور فعل هذا تصبح معلوماتك وبياناتك المالية لدى المُحتال.
- **التطبيقات المخترقة أو التي تقوم بتحميلها من مصادر مجهولة،** أو الروابط الخاصة بتسجيل الدُخول والتي بمجرّد الضغط عليها يتم خرق بياناتك وملفاتك، ويمكن بسهولة سرقة كلمات المرور الخاصة بك أو أرقام البطاقات البنكية التي تمتلكها، وقد تصبح ضحية للابتزاز مقابل دفع المال.
- **الحواسيب خاصة في الشركات والمؤسسات،** والتي يلجأ دائماً القراصنة والمُحتالون إلى خرقها بالبرمجيات والروابط الخبيثة من أجل توقيفها عن العمل أو منع أو حجب الوصول للبيانات مقابل ابتزازك.

- **مواقع التجارة الإلكترونية،** والتي أصبحت مُنتشرة بكثرة وبعضها ما هو إلا واجهة للاحتيال، حيث يطلب منك أن تقوم بالشراء وبعد الدفع لا يصلك المُنتج، أو يصلك مُنتج مُزيّف، وربما أيضًا في الصفحة الخاصة بالدفع يتم سرقة البيانات المالية والمصرفية الخاصة بك.
- **الاحتيال باسم الأعمال الخيرية،** وفيها يدّعي المُحتال أنه يُنظم حملات للتبرّع من أجل الضحايا، أو تقديم المساعدة لشخص ما، وبالطبع إما ترسل الأموال مباشرة، أو يتم سرقة البيانات المصرفية الخاصة بك.



الفصل الثاني: كيفية تنفيذ عمليات الاحتيال عبر الإنترنت

الثغرات الأمنية وعلاقتها بعمليات الاحتيال عبر الإنترنت

- إهمال تحديث أنظمة التسجيل والبرامج والتطبيقات، خاصة التي تقوم بعمليات الحماية.
- إهمال استخدام البرامج المتخصصة في مكافحة الفيروسات والحرص على تحديثها باستمرار.
- استخدام كلمات مرور سهلة ويمكن توقعها بسهولة.
- فتح المرفقات التي تأتي على البريد الإلكتروني، وتحديدًا المجهولة أو التي تبدو غريبة.
- الروابط الإعلانية أو الروابط التي تأتي لك من جهات الاتصال غير المعروفة لديك أو على البريد الإلكتروني.
- المعلومات الشخصية التي يمكن أن تشاركها مع الآخرين؛ سواء من خلال منصات التواصل الاجتماعي، أو من خلال الأشخاص الذين ينتحلون صفة جهة ما رسمية للحصول منك على معلومات.

- عناوين الـ URL التي تأتي بامتدادات غريبة أو غير موثوق بها.
- تسجيل البيانات المصرفية في المواقع الإلكترونية -مواقع التجارة الإلكترونية- خاصة المغمورة منها.



أمن البيانات الشخصية والاحتياال عبر الإنترنت

أمن البيانات هي كُال التدابير التي تُستخدم من أجل حماية وتأمين البيانات ومنع أي وصول غير مسموح به، وذلك لأنه لا بُد من الحفاظ على سرية قواعد البيانات وسلامتها وحمايتها من أي ممارسات خاطئة قد تؤدي إلى تدمير سمة الأشخاص أو المؤسسات والإضرار بهم مادياً ومعنوياً.

ولكي تحمي نفسك من سرقة البيانات عليك أن:

- تتجنب مشاركة أي معلومات شخصية سواء في رسائل البريد الإلكتروني أو على منصات التواصل الاجتماعي.
- استخدام كلمات المرور القوية والمصادقة الثنائية أو متعددة العوامل.
- حماية حساباتك وبطاقاتك البنكية، وذلك بتتبع الأرصدة الخاصة بك، والتأكد من كل حركة تحدث على حسابك، والإبلاغ الفوري عن أي تناقض في حركات السحب.
- تعزيز أمان الأجهزة التي تستخدمها من خلال الحرص على التحديث التلقائي المستمر للأنظمة والتطبيقات، وكذلك تثبيت برامج مكافحة الفيروسات ومكافحة التجسس، وتشغيل جدران الحماية واستخدام كلمات مرور للملفات المهمة.

البصمة الرقمية والاحتياال عبر الإنترنت

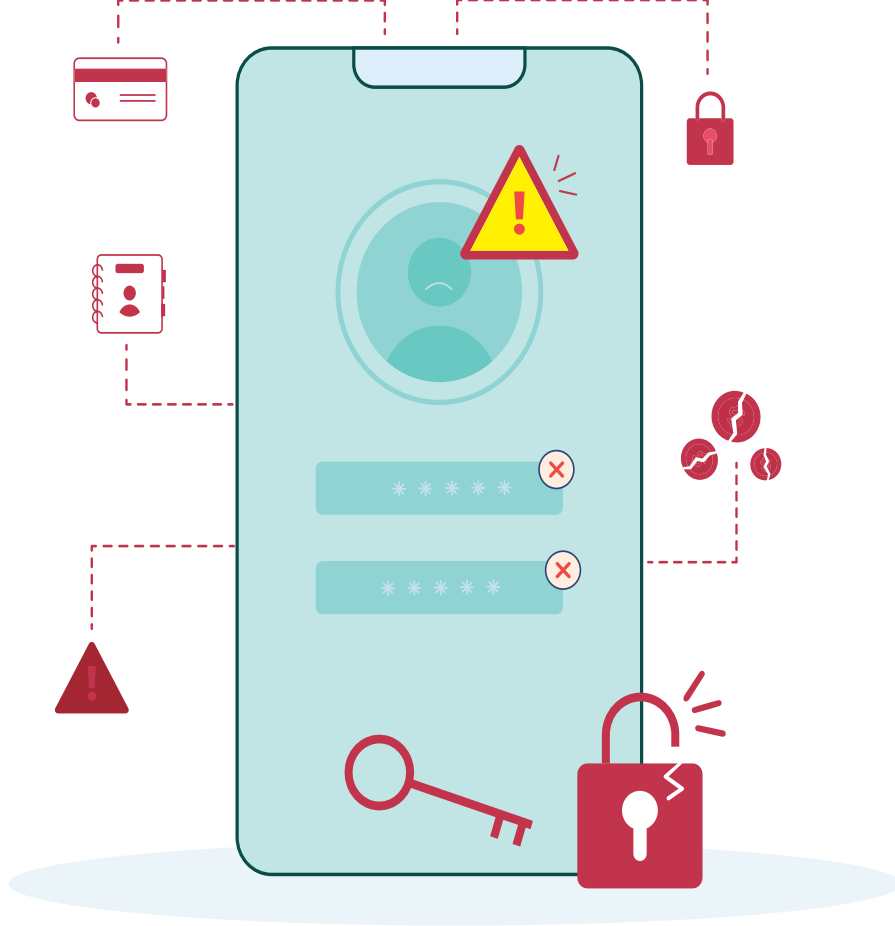
البصمة الرقمية هي الظل الرقمي أو أثر كل البيانات التي تتركها حين تستخدم الإنترنت، وهي تشمل المواقع التي تزورها، ورسائل البريد الإلكتروني التي ترسلها والمعلومات التي تكتبها عن نفسك على منصات التواصل الاجتماعي؛ وذلك لأنك تترك أثراً مع كل استخدام تقوم به، ومهما كانت بساطة ما تقوم به، إلا أنه يعد جزءاً من بصمتك الرقمية، وللأسف هناك علاقة كبيرة بين البصمة الرقمية ومحاولات الاختيال؛ لأن كل ما يتعلق بك يمكن أن يصبح متاحاً للاطلاع العام إن كان على منصات التواصل الاجتماعي خاصة مع عدم تفعيل إعدادات الخصوصية، ويمكنه أن يتحكم في سمةك الرقمية، والتي لا تقل أهمية عن سمةك على أرض الواقع.



الفصل الثالث: كيفية التصرف في حال التعرض للاحتيال عبر الإنترنت

إرشادات الحماية من الاحتيال عبر الإنترنت

- استخدم النسخ القانونية الرسمية من التطبيقات.
- حمل التطبيقات الخاصة بك من المتاجر الرسمية المعروفة، وليس من المواقع مجهولة الهوية.
- احرص على تحديث نظام التشغيل الخاص بالهاتف باستمرار.
- لا تضغط على أي روابط مجهولة المصدر مهما كان الشخص المرسل.
- لا تدخل في تعاملات مع أطراف مجهولة، خاصة فيما يتعلق بالأموال؛ لأنك قد تصبح دون علمك شريكاً في عملية نصب أو محاولة تبييض أموال.
- استخدم البرامج والتطبيقات الخاصة بمكافحة الفيروسات.
- استخدم كلمات مرور قوية ومعقدة.
- لا تتسوق من المتاجر الجديدة أو المجهولة قبل التأكد من سمعتها ومصداقيتها سواء في المنتجات التي تبيعها أو فيما يتعلق بالدفع.





ماذا أفعل عند تعرّضي للاحتيال عبر الإنترنت؟

لا بُدَّ أن تلجأ فوراً إلى والدك أو إلى أحد المُعلّمين في حالة التّعرّض للاحتيال عبر الإنترنت ثمّ التّوجّه إلى إدارة مُكافحة الجرائم الإلكترونيّة بوزارة الدّاخلية للتّصرّف في الأمر وحلّ المُشكلة في أسرع وقتٍ وإنقاذ بياناتك من السرقة، والإبلاغ هنا إن كان سريّاً يساعد الجهات القانونيّة للقبض على المُحتالين، ويحمي غيرك من الصّحايا.

كذلك لا بُدَّ أن تتواصل مع مصرفك في أسرع وقتٍ ممكنٍ، وتطلب إيقاف حسابك تماماً؛ بسبب تعرّضك للاحتيال، كذلك إيقاف كافّة العمليّات المصرفيّة التي قد يقوم بها المُحتالون.

ضرورة مُشارَكَة ما حدث معك على منصّات التّواصل الاجتماعيّ بالتّفاصيل؛ لكي تُعلّم الآخرين الحذر من الأخطاء التي وقعت فيها، وهناك مجموعات مُتخصّصة في كشف الجّناة في هذه القضايا والتي تسمح لك بتبادل الحوار مع المُشاركين للحصول على نصائحهم وحلولهم والتي قد تكون مُفيدة للغاية.

الحَقِيبَةُ التَّدْرِيبِيَّةُ الرَّابِعَةُ



هجوم التصيد الاحتيالي

الفصل الأول: مفهوم التصيد الاحتيالي وأنواعه
الفصل الثاني: كيفية تنفيذ هجمات التصيد الاحتيالي
الفصل الثالث: كيفية التصرف في حال التعرض للتصيد الاحتيالي



الفصل الأول: مفهوم التّصيد الاختياليّ وأنواعه

مفهوم التّصيد الاختياليّ

التّصيد الاختياليّ هو طريقة خطيرة وفعّالة من أجل خرق الأجهزة، ويتمّ فيها استهداف أشخاص أو مؤسساتٍ من خلال روابط أو مُرَقَّقات ضارّة يتمّ إرسالها للمستخدمين، وغالبًا ما يتمّ تحميلها أو النّقر عليها عن طريق الخطأ ومن ثمّ تسرق بياناتهم ومعلوماتهم الشخصيّة.

ووفقًا للدراسات فإنّ 32 % من عمليّات الاختراق على مستوى العالم هي عمليّات تصيد اختياليّ، وحوالي 64 % من المؤسسات والمنظّمات تتعرّض للتّصيد الاختياليّ مرّة واحدة على الأقلّ في تاريخها.

أنواع وأشكال التّصيد الاحتياليّ

- **الهندسة الاجتماعية:** وهي هجوم قائم على خداع الضحايا للقيام بفعل سريع عبّر معلومات مُزيّفة وخادعة، وغالبًا ما يتمّ انتحال صفة مؤسسة رسمية وجهات ثقة لخداع المُستخدم ودفعه للتّحرك والتّصرّف بسرعة وبدون تفكير أو تركيز.
- **مُحاكاة الروابط:** وهذه الطريقة تقوم بعَمَل نَسَخ مُزيّفة للمواقع الرّسميّة، وتشبه تلك المواقع المُزيّفة المواقع الأصليّة وستبدو من الوَهلة الأولى أنّها شرعيّة تمامًا، وقوْر الدّخول إلى الموقع والنّقر عليه يطلّب منك معلوماتك، وبالطّبع حين تُدخِل المعلومات تصبح في يد اللّص، وبالتالي يمكنه استخدامها في أيّ غرض يريد حتى لو كان لأغراض شخصيّة ضارّة.
- **التّصيد الاحتياليّ من خلال البريد الإلكترونيّ:** وهي الطريقة الأكثر شُيوعًا ويتمّ فيها إرسال بريد إلى مُستخدم ما معه مُرفقات أو روابط. وبمجرّد الضّغط عليها يتمّ السيطرة على الجهاز واختراقه.
- **برمجيّات الفدية:** وتلك برمجيّات شائعة للغاية ويستخدم فيها برمجيّات متخفية غالبًا ما تأتي في صورة مُرفق مَوْثوق به وقوْر الضّغط عليها يتمّ تحميلها على الجهاز، وقد تتسبّب في تعطيل الأنظمة وسرقة البيانات مُقابل فدية بدلًا من تدميرها.

- **التّصيد الاحتياليّ المُوجّه:** وفيه يتمّ استهداف أشخاص مُعيّنين من خلال المعلومات التي تمّ جَمْعها بالبحث عنهم ومُراقبة البصمة الرّقميّة الخاصّة بهم.
- **التّصيد الاحتياليّ المُوجّه لكبار الشخصيّات (تصيد الحيتان):** خاصّة مع السّياسيين أو رجال الاقتصاد أو المشاهير، وغالبًا ما يتمّ خَرْق البيانات وسرقتها من أجل استغلالها في الابتزاز وتحقيق المكاسب الماليّة.
- **التّصيد عبْر الرّسائل النصّيّة:** ويتمّ من خلال رسائل قصيرة تأتي في هيئة نُصوص وعادةً ما تكون شخصيّة لإقناع المستلم الضّغط على الرّابط، أو القيام بأمر ما، ومن خلال هذا الأمر يتمّ اختراق الجهاز.
- **التّصيد الصّوتيّ:** وهو أحد أشكال التّصيد الاحتياليّ التي تعتمد على الدّكاء الاصطناعيّ؛ حيث يتمّ توليد أصوات أشخاص بعينهم لإرسال رسائل للضحايا لإقناعهم بتحويل الأموال أو الإفصاح عن معلومات مُعيّنة.

الفصل الثاني: كيفية تنفيذ هجمات التصيد الاحتيالي

الثغرات التي يستغلها مُنفذو هجمات التصيد الاحتيالي

هناك عدة طرق تُستخدم لتنفيذ هجمات التصيد الاحتيالي، وهي:

- **التصيد بناءً على الحاجة:** وهنا يتم استغلال حاجة الضحية لأمر ما أو خلق حالة من الوهم لإقناع الضحية بعمل، أو اتخاذ إجراء ما دون التفكير فيه لأكثر من مرة، كإرسال رابط لهدية أو لإجازة مدفوعة، وبالطبع ينقر المستلم وقد يُسجل بياناته وهو لا يعرف أنه بهذه الطريقة يُسلم بياناته للمتصيدين.
- **الثقة الزائفة:** والتي غالباً ما تحدث بسبب انتحال المتصيدين لهويات معينة جديرة بذلك، ولا يشترط أن تكون لأشخاص، بل يمكن أن تكون لجهات مثل Google مثلاً أو تطبيق Facebook، ومن خلال هذا الانتحال يحصل المتصيد على المعلومات بكل سهولة.
- **التلاعب العاطفي:** واستخدام أساليب الضغط النفسي لإقناع الضحايا بالتصرف الفوري دون تفكير، وغالباً ما يتم انتحال صفة مؤسسة أو مصدر مألوف للمستخدم، وغالباً ما يتم التركيز على مشاعر الخوف والقلق؛ لأن الناس يميلون لاتخاذ قرارات سريعة لإنقاذ أنفسهم.





الأخطاء التي يرتكبها مُستخدمو الإنترنت

- التَّصرُّفُ بِسُرْعَةٍ وبدون تفكير.
- عدم التَّأكُّد من صحَّة الأمر المطروح أمامهم، سواء كان رابطًا مُرسلًا إليهم، أو موقعًا إلكترونيًا يتطلَّب تسجيل الدُّخول، أو حتى مُكالمة صوتية تطلب منهم بيانات مُعيَّنة.
- الضُّغط على المُرفقات أو الرُّوابط التي تأتي من مصادر مجهولة أو غير موثوقة.
- نَشْر المعلومات الشَّخصية والسَّريَّة على حسابات التَّواصل الاجتماعيِّ.
- تجاهل تأمين الحسابات بكلمات مرور قوية ومُعقَّدة.

البَصْمَةُ الرِّقْمِيَّة والتَّصِيدُ الِاخْتِيَالِيَّ

تَكْمُنُ خُطُورة البَصْمَةِ الرِّقْمِيَّة في أنَّها بيانات دائمة ومُتاحة خاصَّة إن كانت على مواقع التَّواصل الاجتماعيِّ كُلِّ ما تشاركه عن نفسك وعن المحيطين بك، ويمكن لجهات العمل التَّحقُّق من بَصْمَتِكَ الإِلِكْترُونِيَّة بِسُهولة، كذلك يمكن استغلال بَصْمَتِكَ الإِلِكْترُونِيَّة في الإضرار بك أو استغلالها من أجل ابتزازك وتهديدك وتَشْوِيهِه سُمْعَتِكَ أو في أسوأ الظُّروف سرقة هُويَّتِكَ أو إنشاء هُويَّة مُزيِّفة بِتَفْس اسمك وبياناتك.

الفصل الثالث: كيفية التصرف في حال التعرض للتصيد الاحتيالي

إرشادات الحماية من التصيد الاحتيالي

- لا تثق أبدًا في رسائل البريد الإلكتروني التي تطلب منك بياناتك أو تطلب منك الضغط على رابط أو تحميل مرفقات، كل ما عليك فعله أن تقوم بمحوها تمامًا في نفس الوقت.
- الجِرس على تثبيت برامج مكافحة الفيروسات والبرمجيات الضارة، وتحديثها باستمرار.
- كتابة كلمات مرور قوية، وتغييرها بين الحين والآخر، وعدم استخدام نفس كلمة المرور للحسابات المختلفة.
- عدم مشاركة المعلومات الشخصية على منصات التواصل الاجتماعي؛ فمشاركة هذه المعلومات قد تؤدي إلى وقوعك ضحية للتصيد الاحتيالي.

حماية البيانات من القرصنة

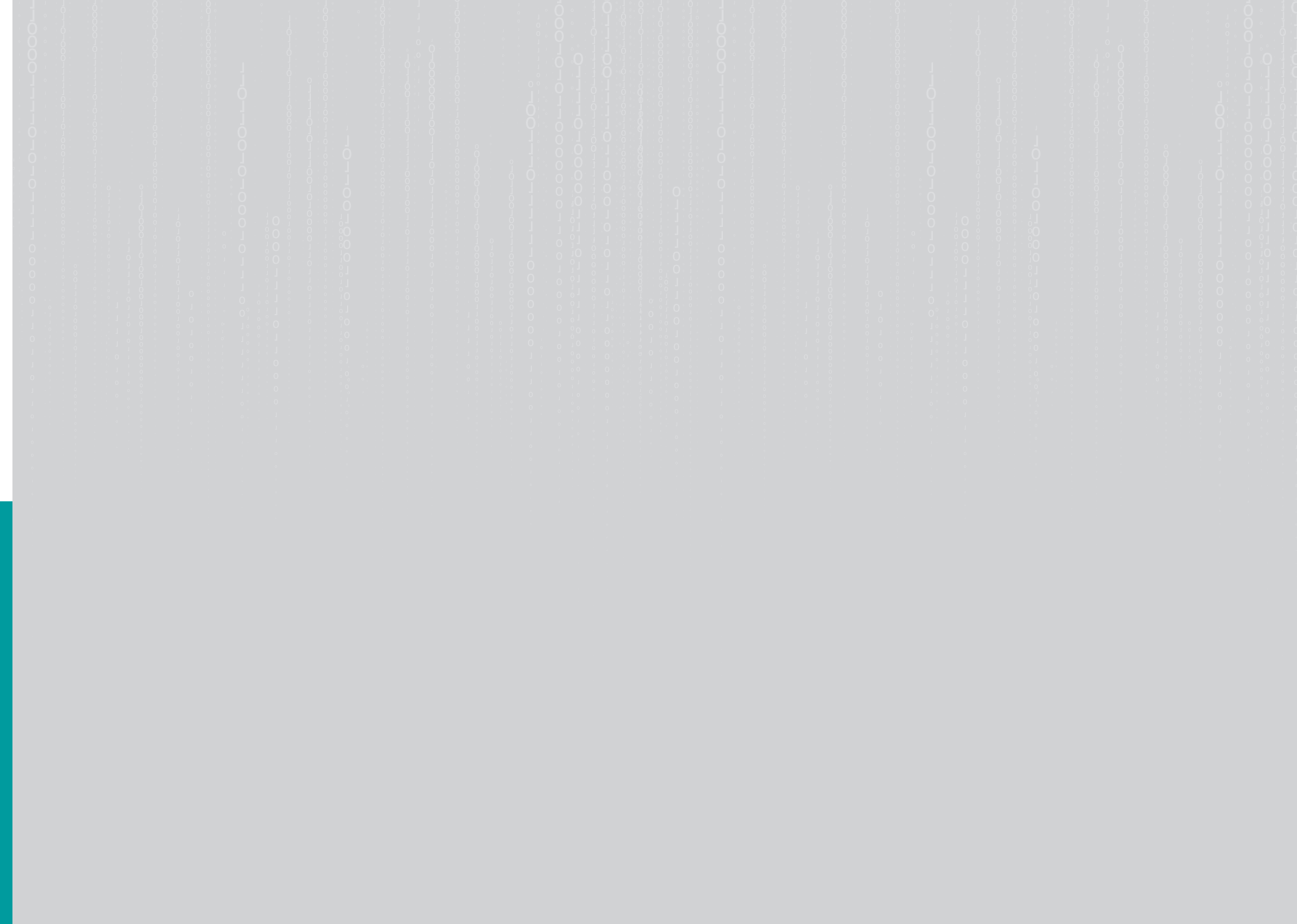
لكي تحمي بياناتك من القرصنة يجب اتباع الآتي:

- تثبيت برامج الحماية والجِرس على تحديثها في أسرع وقت، وكذلك أنظمة التشغيل.
- تأمين الأجهزة المتصلة بالإنترنت، واستخدام كلمات مرور قوية ومعقدة.

- التأكد من تفعيل جدار الحماية على أجهزتك.
- تشفير القرص الصلب وذلك لتحويل بياناتك إلى أكواد غير قابلة للقراءة.
- تجنب الدخول من شبكات الإنترنت العامة.
- عدم إهمال مسح البيانات الخاصة بك من الأجهزة القديمة.
- استخدام كلمات مرور قوية ومعقدة لحساباتك الإلكترونية المختلفة.
- الاستعانة بخدمة المصادقة الثنائية.
- يمكنك الاستعانة بشبكة الضيوف في منزلك؛ لكي تحمي نفسك من المتطفلين.

كيف أتصرف عند تعرضي للتصيد الاحتيالي؟

في حالة التعرض للتصيد الاحتيالي عليك أن تتوجه فورًا إلى الوالدين أو إلى أحد المعلمين بالمدرسة لمساعدتك في التواصل المباشر مع إدارة مكافحة الجرائم الإلكترونية بوزارة الداخلية لتقديم يد المساعدة المتخصصة، وتقديم كافة المعلومات التي تعرفها؛ لكي يتمكنوا من إيقاف المخترق والقبض عليه.



الحَقِيبَةُ التَّدْرِيبِيَّةُ الْخَامِسَةُ



حُقوقُ التَّأليفِ والنَّشرِ

الفصل الأول: مفهوم حُقوق التَّأليف والنَّشر الإلكتروني
الفصل الثاني: أشكال التَّعدِّي على حُقوق النَّشر الإلكتروني

[illegible]

الفصل الأول: مفهوم حقوق التأليف والنشر الإلكتروني

حقوق النشر هي تلك الحقوق التي يمتلكها الأفراد أو المؤسسات عند صنعهم أي نوع من أنواع المحتوى، بشرط أن يكون المحتوى أصلياً غير منسوخ أو مسروق، ويتم الاحتفاظ به في وسيط مادي، ومالك حقوق النشر والطبع لديه الحق الحصري لاستخدام العمل أو المحتوى، ويمكنه بيع أو إعطاء الآخرين الإذن لاستعمال هذا العمل أو المحتوى.

أنواع حقوق التأليف الإلكتروني والمؤسسات الدولية الرعاية لها

- الأعمال الصوتية المرئية مثل برامج التلفزيون والأفلام والفيديوهات.
- التسجيلات الصوتية والمؤلفات الموسيقية.
- الأعمال المكتوبة مثل المحاضرات والمقالات والكتب.
- الأعمال المرئية مثل اللوحات الفنية والملصقات والإعلانات.
- الألعاب الإلكترونية وبرامج الحاسوب.
- الأعمال الدرامية والأعمال المسرحية.

وتعد المنظمة العالمية للملكية الفكرية WIPO الجهة العالمية الأساسية المختصة في خدمة الجمهور من أفراد وشركات لحماية حقوق الملكية الفكرية وحقوق الطبع والنشر، وهي المنتدى العالمي لسياسة الملكية الفكرية، وطورت العديد من الدول الفكرة نفسها لمؤسسات محلية هدفها حماية المنتجين والمحتوى والإنتاج الفني الخاص بالأفراد والشركات.





الفصل الثاني: أشكال التّعدي على حقوق النشر الإلكتروني

- تقليد الأعمال الأصلية وبيعها وتعريف الجمهور أنّها مُقلّدة.
- التقليد والبيع أو التداول مع المُنتجين الآخرين حتى ولو كانوا خارج البلاد.
- نشر المُحتويات والأعمال على شبكة الإنترنت دون إذن كتابي من المؤلف أو صاحب الحق.
- استخدام المُحتوى أو أجزاء منه دون الحصول على إذن صاحب المُحتوى حتى لو تمّ ذكر اسم صاحب الحقوق عليها.
- إزالة المُحتوى الأصلي أو تعييبه أو تعطيله من أجل نشر المُحتوى المُزيّف.
- إزالة اسم المُنتج أو صاحب الحقوق أو المؤلف من العمل الفني.

كيفية تنفيذ التعديلات على حقوق التأليف والنشر الإلكتروني

- التصوير أو المسح الضوئي للنماذج الرقمية أو نسخ أو لصق أي أجزاء من العمل الأصلي دون الحصول على إذن المؤلف أو المنتج.
- البريد الإلكتروني وهو النوع الأقل استخدامًا ويحدث حين يكون لدى شخص ما حقوق استخدام منتج أو محتوى بشكل حصري فيقوم ببيعه أو توزيعه من خلال البريد الإلكتروني وإعادة توجيهه لأشخاص آخرين.
- الشبكات، وذلك حين يتم انتهاك حقوق النشر على شبكة عامة أو خاصة؛ لكي يتمكن الكل من رؤية المحتوى دون العودة للمؤلف أو صاحب الحق الأصلي.
- مشاركة الملفات عن طريق تحميل أو تنزيل ملفات على مواقع الإنترنت؛ ليتمكن الجميع من إعادة تحميلها ونسخها.
- القرصنة والتزوير من خلال عمل نسخ من المحتويات الأصلية -نسخ مُقلدة- وبيعها للآخرين حتى وإن كانوا على معرفة بأن هذا المحتوى غير أصلي.

أساليب الحماية من التعدي على حقوق النشر الإلكتروني

- أولًا: الحصول على ترخيص سواء كان المحتوى صورة أو مقطعًا أو صوتًا أو أيًا كانت طبيعته.

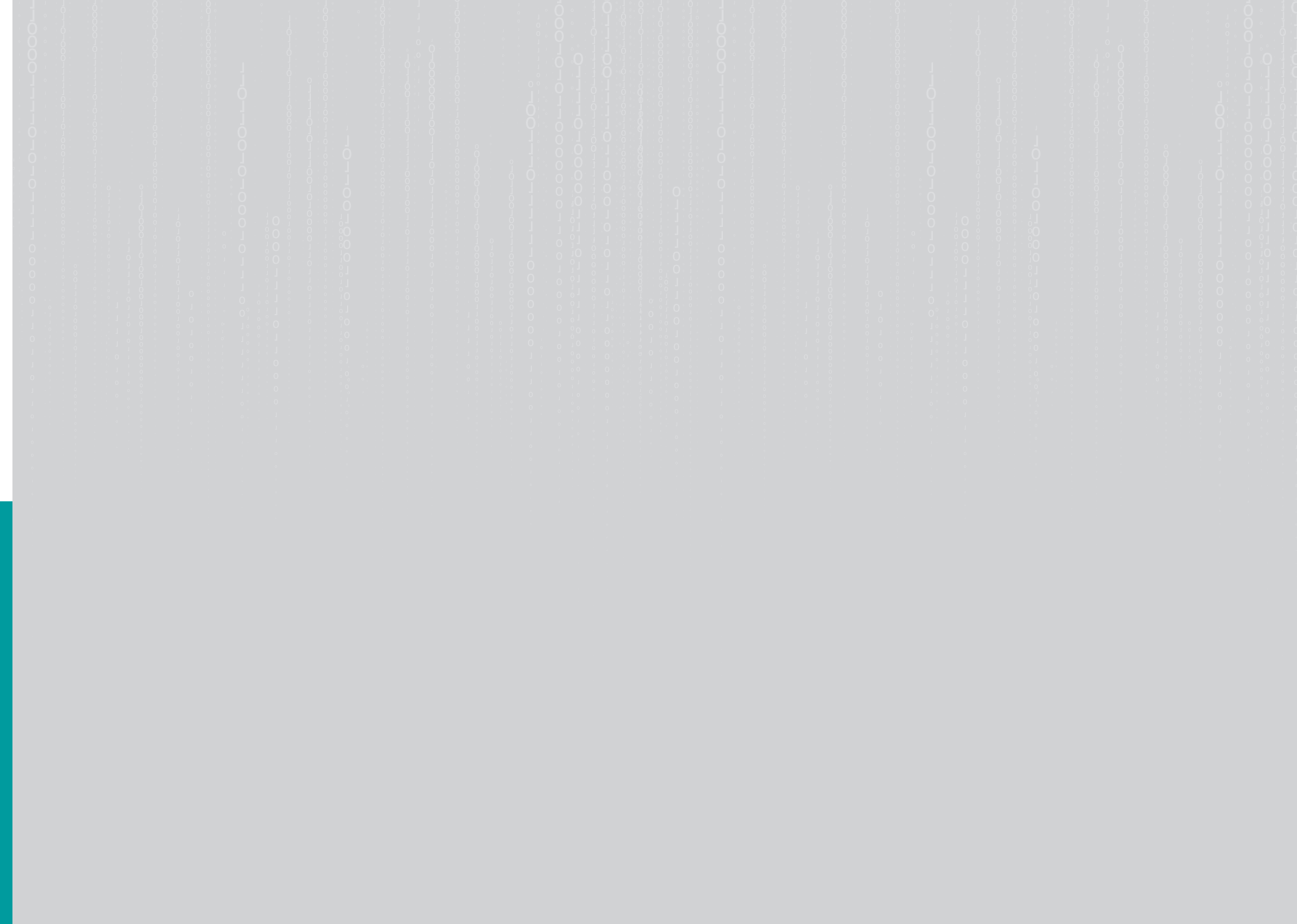
- ثانيًا: تضمين شارة الحماية، والتي تُوفر الحماية للمحتوى بشكل مجاني، ويمكن وضعها على المواقع الإلكترونية، وقد تحمي المحتوى من محاولات النسخ والقرصنة.
- ثالثًا: التحقق من السرقة الأدبية من خلال المواقع التي تتحقق من نسخ المحتوى.
- رابعًا: بالنسبة للمستخدم لا بد أن يتجنب المشاركة في هذه السرقة؛ لأنها تضر بالمنتج والفنان على المستوى المادي والمعنوي، وتجعل الفضاء الإلكتروني بيئة غير آمنة.





المرحلة الثانية

في هذه المرحلة سيتم تقديم التدريب الرقمي من خلال ثلاثة محاور، هي بروتوكول IMAP4، وروبوتات الشبكة العالمية، وسياسة أمان المحتوى، وفيما يلي تبيان لأهم المعلومات التي سيتم تقديمها في هذه المحاور.



الحَقِيبَةُ التَّدْرِيبِيَّةُ السَّادِسَةُ



بروتوكول IMAP4

الفصل الأول: مفهـوم بروتوكول (IMAP4)

الفصل الثاني: كيفية عمل بروتوكول (IMAP4)





يُعدّ بروتوكول (IMAP4) أو بروتوكول (POP3) من الطُّرُق الأساسيَّة للوصول إلى البريد الإلكترونيّ، ويُعدّ البروتوكول (IMAP4) هو الأسلوب الأفضل، خاصَّةً إن كنت تعتمد على أكثر من جهازٍ للتحقق من رسائل البريد الإلكترونيّ الخاصَّة بك، مثل الهاتف الذكيّ أو الحاسب المحمول أو الحاسوب اللّوحيّ.

الفصل الأوّل: مفهّوم بروتوكول (IMAP4)

بروتوكول (IMAP4) هو البروتوكول المسؤول عن الوصول إلى رسائل البريد الإلكترونيّ الخاصَّة بك في أيّ مكانٍ ومن أيّ جهازٍ، كل ما عليك فعله أن تقوم بتسجيل الدُّخول، وبعدها تجد رسائلك دون الحاجة إلى تنزيلها أو تحميلها أو تخزينها على الجهاز الذي تستخدمه، وبالتالي يمكنك قراءة البريد من البريد الإلكترونيّ في أيّ وقتٍ ومن أيّ جهازٍ متّصل بالإنترنت.

ويتميّز هذا البروتوكول بأنّه لا يقوم بتحميل المرفقات بشكلٍ تلقائيّ، ولكن عليك الضّغط عليها لكي يتمّ تنزيلها أو فتحها وهو ما يُوفّر للمستخدم سرعة أكبر وقُدرة على استقبال أعدادٍ أكبر من البريد دون الحاجة لمساحة تخزينيّة على الجهاز المُستخدم.

أهميّة بروتوكول (IMAP4)

تُكمن أهميّة هذا البروتوكول في كونه يُوفّر إمكانية فتح البريد الإلكتروني في أيّ مكانٍ ومن أيّ جهازٍ، سواء كان جهازًا خاصًا بك أو لصديق أو لزميل، كما أنّه يُوفّر لك عنصر السرعة في الاستجابة -الوصول والفتح- لأنّ المرفقات لا يتم تنزيلها بشكلٍ تلقائيٍّ، ولكن بعد أن تضغط عليها، كما أنّه لا يحتاج إلى مساحة تخزينيّة على الجهاز لأنّه بالكامل موجود على الإنترنت. وهو ما يجعل هذا البريد يحتفظ بالرسائل طالما لم تحذفها أنت بنفسك؛ لأنّه لا يستهلك مساحة مثل البروتوكولات الأخرى.

وبخلاف هذا يُتيح هذا البروتوكول للمستخدم أن يفتح بريده الإلكتروني على أكثر من جهازٍ في الوقت نفسه، بمعنى أنّه يمكنك تحميل تطبيق البريد الإلكتروني أو فتحه من المتصفح على جهاز هاتفك المحمول، وفي الوقت نفسه على الحاسوب.

الفرق بين بروتوكول (IMAP4) وبقية البروتوكولات المتبعة في البريد الإلكتروني

بروتوكول (IMAP4) ليس البروتوكول الوحيد الذي يُستخدم لإدارة البريد الإلكتروني، فهناك أيضًا بروتوكول (POP3) وهذا البروتوكول من البروتوكولات القديمة والتي صُممت في الأساس ليتم فتح البريد على جهازٍ واحدٍ فقط، وبالتالي لا يدعم المزامنة ثنائية الاتجاه مثل البروتوكولات الحديثة، ويعمل فقط بمزامنة

البريد أحاديّة الاتجاه، وبالتالي يسمح للمستخدمين بتنزيل رسائل البريد الإلكتروني من الخادم إلى العميل، ولذلك يفتقر إلى معظم الوظائف الأساسية التي يمكن العثور عليها في الخدمات الحديثة.

فلا يمكن ل-POP3 أن يُتيح لك قراءة الرسائل من أكثر من جهازٍ، وبالتالي يمكنك فقط قراءة رسائلك من جهازٍ واحدٍ فقط لا غير، كما أنّه لا يسمح بحفظ الرسائل إلا على جهازٍ واحدٍ فقط -الذي يعمل من خلاله- ومن مميزات هذا البروتوكول وعيوبه في الوقت نفسه أنّه يقوم بتحميل الرسائل الخاصة بك، وبالتالي يُتيح لك قراءة الرسائل من جديدٍ حتى وإن كان جهازك غير متّصل بالإنترنت، ولكن في الوقت ذاته يستهلك مساحة تخزينيّة كبيرة خاصّة فيما يتعلّق بالمرفقات.



الفصل الثاني: كيفية عمَل بروتوكول (IMAP4)

حين يتم إرسال رسالة بريد إلكتروني يقوم البروتوكول (SMTP) وهو بروتوكول نقل البريد البسيط بتحديد كيفية إرسال رسائل البريد الإلكتروني، وبعدها:

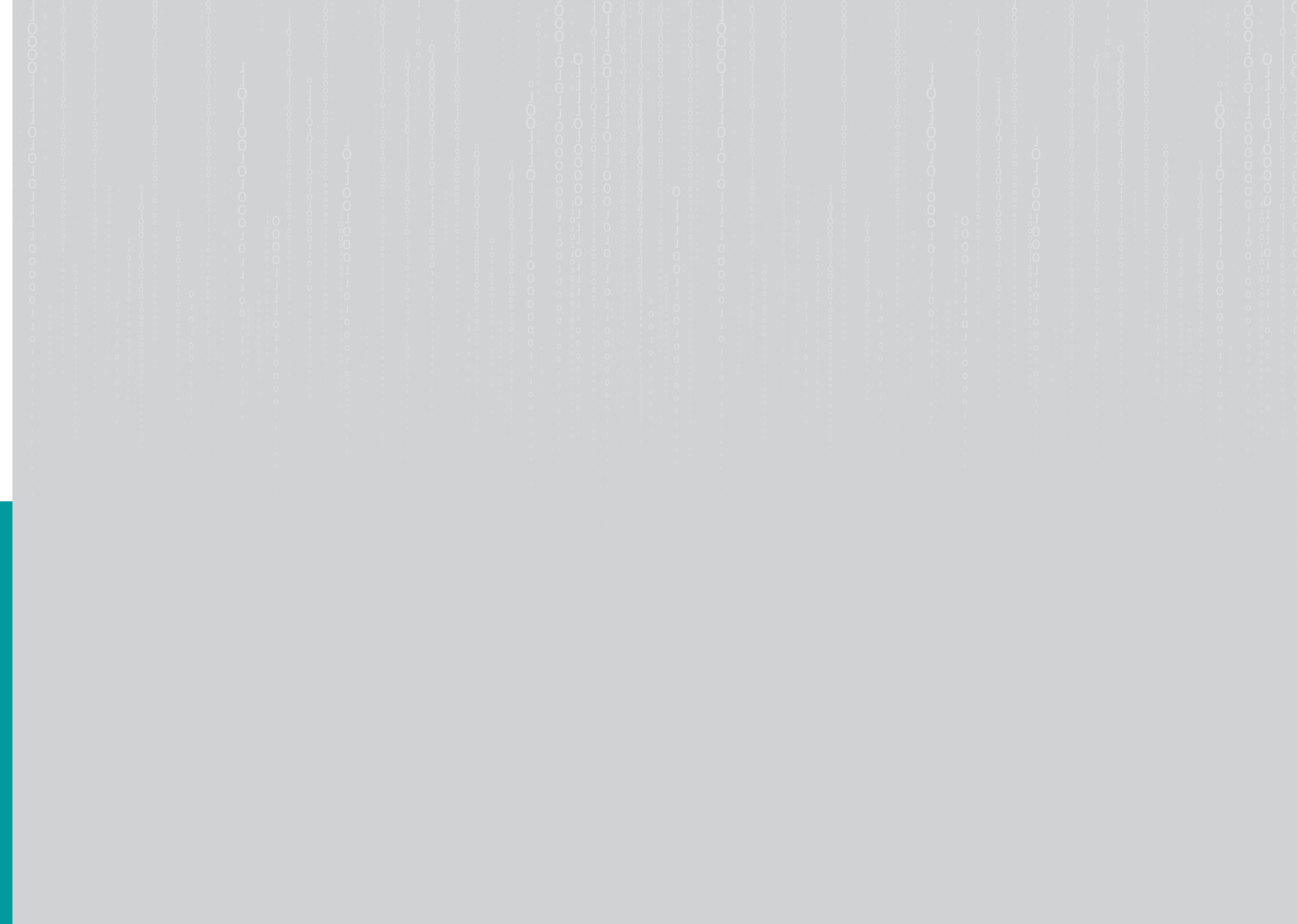
1. يتم إعداد اتصال بروتوكول التحكم في الإرسال (TCP) بين العميل وخادم البريد الإلكتروني، وهذا البروتوكول مسؤول عن معرفة وتجهيز الاتصال تمهيدًا لنقل رسالة بريد إلكتروني.
2. بعدها يرسل العميل سلسلة من الأوامر إلى الخادم ومن ضمن هذه الأوامر البريد نفسه.
3. يستخدم خادم البريد الإلكتروني برنامج الخاَص المُسمَّى وكيل نقل البريد (MTA) لكي يتحقق من سجل نظام اسم المجال (DNS) للبريد الإلكتروني وبعده العثور على عنوان IP المُستلم.
4. يترجم (MTA) سجل DNS إلى عنوان IP من أجل معرفة مكان إرسال رسائل البريد الإلكتروني.
5. وأخيرًا يبحث (SMTP) عن سجل تبادل البريد MX المرتبط باسم مجال المستلم، وإن كان هناك سجل MX فسيتم إرسال البريد الإلكتروني إلى خادم البريد الإلكتروني المقابل له.

بروتوكول (IMAP4) وتنظيم البريد الإلكتروني وحمايته

من أهم مميزات بروتوكول (IMAP4) أنه يُخزّن البريد افتراضيًا أو على الخادم الافتراضي، لذا إن حدثت أي مشكلة، على سبيل المثال «اختراق الخادم» فلا مشكلة ولا داعي للقلق؛ لأنّ بكلّ بساطة هذا البروتوكول يقوم بالتّخزين على الخادم الافتراضي، وبالتالي لن تختفي رسائل البريد الإلكتروني، على عكس POP3 والذي تختفي الرسائل من عليه في حالة تلف الجهاز الذي تمّ التّحميل عليه أو فقده لأيّ سبب.

أيضًا يُوفّر هذا البروتوكول طبقة أمان إضافية من خلال تسجيل الدخول بكلمات مرور واسم المُستخدم، ويمكن تفعيل خاصيّة التّحقق بخطوتين بسهولة، ويعتمد البروتوكول على تشفير كلمات المرور باستخدام مُعادلات رياضيّة تجعل كلمات المرور مُعقّدة، ولا يمكن للمُهاجمين فهمها بمجرد قراءتها.





الحقيبة التدريبية السابعة



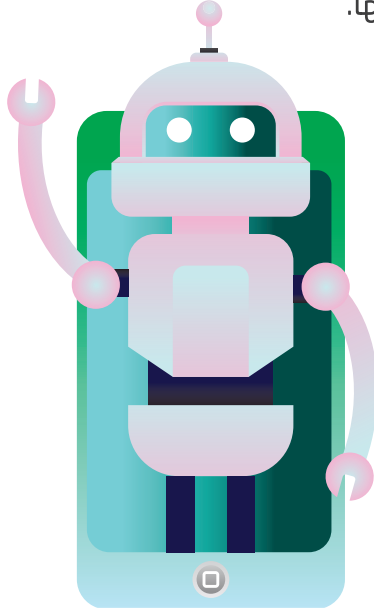
روبوتات الشبكة العالمية

الفصل الأول: مفهوم روبوتات الشبكة العالمية وأنواعها
الفصل الثاني: آلية عمل روبوتات الشبكة العالمية وفائدتها

مفهوم روبوتات الشبكة العالمية

الروبوتات هي برامج تقوم بعددٍ من المهام بطريقة آلية وبشكلٍ مُتكرّرٍ ومُحدّدٍ مسبقًا، وبالطبع تتميز عن البشر بسرعتها وإمكانية استغلالها في كثيرٍ من المهام، على رأسها فهرسة محرّكات البحث وصفحات الويب وكذلك خدمة العملاء. **وتساعد الروبوتات الشركات بكثيرٍ من الطُّرق، منها:**

- تمديد ساعات العمل وتوفير النِّفقات.
- تحسين الموارد وزيادة الوصول إلى شرائح أكبر من الجمهور.
- القيام بالمهام المُملة والمُتكرّرة.
- تلافي الخطأ البشريّ الوارد في حالة تكرار نفس المهمة أكثر من مرّة.
- جَمع البيانات وتحليلها.



روبوتات الشبكة العالمية أو ما يُعرّف بـ Bots بوتات الإنترنت أو روبوتات الويب، كلّها مسمّيات تُعبّر عن تلك البرامج التي تقوم بالمهامّ التلقائيّة على الإنترنت، وهذه المهامّ مُتنوّعة بين البسيطة والمُركّبة، ولكنّها مُتكرّرة، وبالتالي تُعدّ تلك الروبوتات مهمّة لأنّها تعمل بمعدّل أعلى من المعدّل الذي يعمل به الإنسان وحده، وأكبر مهمّة للبوتات هي فهرسة صفحات الإنترنت، من خلال جلب وتحليل المعلومات من الخوادم بشكلٍ تلقائيٍّ وبسرعةٍ عالية، ومن ثمّ يتمّ مراجعة البيانات الموجودة في الصفحات وفهرستها إن كانت تتوافق مع القواعد التي تحكّم سلوك البوت على الخادم.

الفصل الأوّل: مفهوم روبوتات الشبكة العالمية وأنواعها

روبوتات الشبكة العالمية هي برامج تعمل بسرعة كبيرة وتقوم بمهامّ بسيطة ومُركّبة معروفة مُسبقًا وبسرعةٍ كبيرة، وأكبر مهمّة تقوم بها هي فهرسة صفحات الويب، وفي العادة، تُحاكي البوتات سلوك البشر، ولكنّها أسرع كثيرًا من البشر؛ لأنّها آلية، وبالتالي يمكنها تنفيذ كثيرٍ من المهامّ المفيدة، وتُستخدم كذلك في خدمة العملاء.

وتُعدّ روبوتات الشبكة العالمية أدواتٍ رقميّةٍ يمكن استخدامها في الأمور الجيدة أو السيئة، ومنها بوتات ضارّة، فهي في الأساس برمجيات، وبالتالي يمكن استغلالها واختراقها.

أنواع روبوتات الشبكة العالمية

هناك عدّة أنواع من البوتات، وهي تنقسم ما بين جيّدة وخبيثة، إليك أنواع روبوتات الويب النّافعة والضّارة:

الروبوتات النّافعة

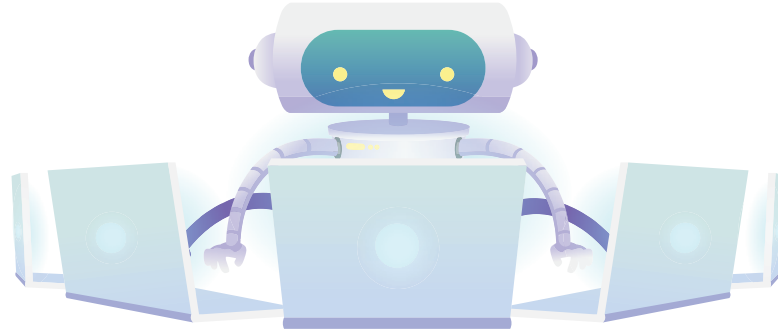
- **روبوتات الدّردشة لخدمة العملاء:** وهي روبوتات تُحاكي المُحادثات البشريّة، وتعتمد على الذّكاء الاصطناعيّ، وتستخدمها أغلب الشّركات للردّ على استفسارات العملاء.
- **مُتتبّعات الويب:** وهذا النوع يُطلَق عليه العناكب، وهي روبوتات محرّك البحث التي تفحص صفحات الويب وثقُورِستها، لذا تساعد محرّكات البحث على تقديم تجربة بحث أفضل من خلال استخراج البيانات وفهم هيكل المحتوى ومدى الملاءمة.
- **أدوات استخراج بيانات الويب:** ويُطلَق عليها المُتتبّعات، وهي الأدوات التي تساعد في فحص محتوى مُحدّد على الإنترنت ونزله، وتستخدمها الشّركات خاصّة في التّجارة الإلكترونيّة من أجل رّد أسعار المُنتجات المباشرة على منصات البيع بالتّجزئة.

- **روبوتات التّسوّق:** وهي روبوتات متخصّصة في رّد أسعار المُنتجات على عددٍ من المواقع الإلكترونيّة من أجل مساعدة العملاء في العثور على أفضل الصّفقات.
- **روبوتات المراقبة:** وهي المتخصّصة في الحدّ من التّعرّض للحوادث الأمنيّة، عن طريق فحص الأنظمة لإيجاد الأخطاء أو التّرمجّيات الخبيثة، ومن ثمّ تنبيهك إلى الأنشطة غير العاديّة من خلال جَمع بيانات تفاعل المُستخدمين وحركة مرور الويب وتحليلها.
- **روبوتات المعاملات:** وهذا النوع يتأكّد من صحّة الأشياء، مثل صحّة تسجيل تفاصيل الدّفع قبل إنهاء المعاملات، خاصّةً على مواقع التّجارة الإلكترونيّة، والتّحقّق من دقّة تفاصيل البطاقات البنكيّة والائتمانيّة والمعلومات الشّخصيّة في عمليّات السّداد، ويُعدّ هذا النوع من البوتات الآمنة للغاية من أجل حماية البيانات الماليّة والحسّاسة.

أما عن الروبوتات الخبيثة فتشمل:

- **روبوتات التنزيل:** وهي روبوتات مُبرمجة على التنزيل التلقائي للبرامج والتطبيقات، وتُعطي تصنيفًا خاطئًا للتطبيقات التي تستعين بها لاكتساب مزيد من الظهور وجذب المشتركين بطرق غير شرعية.
- **روبوتات البريد العشوائي:** وهي الروبوتات التي تستخرج العناوين من الإنترنت ثم تقوم بعمل قوائم كبيرة من العناوين وتُرسل عليها رسائل لأعداد كبيرة من المستخدمين، ويمكن أيضًا لهذا النوع أن يُنشئ حساب بريد إلكترونيًا ليقوم بالنشر على المنتديات ومنصات التواصل الاجتماعي، وهذه الروبوتات غالبًا ما تُستخدم لحث الناس على الضغط على روابط مواقع مُختَرقة أو تنزيل ملفات ضارة.
- **روبوتات التذاكر:** وهذا النوع موجود بشكلٍ حصريٍّ على المواقع التي تعمل في بيع التذاكر، وتقوم بشراء التذاكر بأسعار قليلة، ثم بعد انتهائها تُعيد البيع من جديد ولكن بأسعار أعلى، وتُعدّ هذه الروبوتات في بعض البلاد من الممارسات غير الأخلاقية.
- **روبوتات حجب الخدمة الموزعة DDOS:** وهي من البرمجيات الخبيثة التي تُستخدم من أجل إجراء هجوم موزع لحجب الخدمة. وهجوم حجب الخدمة الموزع هو محاولة الهدف منها الإضرار بنظام مُستهدف مثل موقع إلكتروني أو تطبيق محدد.

- **الروبوتات الاحتيالية:** وهي الروبوتات التي يُطلق عليها أحيانًا روبوتات النقر الاحتيالي، التي تستخدم الذكاء الاصطناعي لثحاكي السلوك البشري من أجل تنفيذ الاحتيال الإعلاني؛ حيث تُستخدم للضغط على الإعلانات في المواقع الإلكترونية من أجل تحقيق عائدات من الإعلان للنّاشر.
- **روبوتات مشاركة الملفات:** وتلك الروبوتات تعتمد على تسجيل مصطلحات البحث المُتكررة على التطبيقات أو برامج المراسلة أو محرّكات البحث، ثم تقديم توصيات بروابط غير شرعية أو غير مرغوب فيها لملفات أو مواقع إلكترونية خبيثة.
- **روبوتات الوسائط الاجتماعية:** وهي الروبوتات التي تخلق نشاطًا زائفًا على منصات التواصل الاجتماعي أو الوسائط الاجتماعية، مثل الحسابات، المُتابعات، الإعجابات، أو التعليقات المُزيّفة، وثحاكي تلك الروبوتات سلوك ونشاط البشر على منصات التواصل الاجتماعي، لكنّها على الأغلب تقوم بإرسال محتويات غير مرغوب فيها، أو نشر معلومات غير صحيحة، أو دعم وتعزيز شعبية أمرٍ ما أو شخصٍ ما.



- **شبكة الروبوتات Botnet:** وهذا النوع عبارة عن مجموعة من الروبوتات الخبيثة التي تعمل معًا بطريقة مُنَسَّقة في مهام تتطلب أحجامًا كبيرة من طاقة الحوسبة والذاكرة، وتستخدم على الأغلب من أجل تقليل التكاليف أو توحيد آليات إدارة المهام بصورة مركزية؛ لأن شبكة الروبوتات يتم تثبيتها على أجهزة متصلة بالشبكة -تتبعي إلى الآخرين-، ومن ثم يمكن التحكم في تلك الشبكة عن بُعد والتخطيط للاستفادة منها كطاقة حوسبة دون دفع نظير أو مقابل لها.

الفصل الثاني: آليّة عمل روبوتات الشبكة العالمية وفائدتها

كيف تعمل روبوتات الشبكة العالمية؟

يمكن للبوتات أن تتواصل مع بعضها باستخدام الإنترنت، ويمكنها أيضًا المراسلة الفورية، أو التّغريد، من خلال بروتوكول الدّردشة عبر الإنترنت IRC، وتتكوّن البوتات من مجموعات من الخوارزميات التي تساعد على تنفيذ المهامّ التي ستقوم بها، ويتمّ تصميم أنواع البوتات حسب المهامّ التي ستقوم بها والطّرق المختلفة التي ستستخدمها في القيام بالمهامّ، على سبيل المثال بوتات المُحادثة:

- تتفاعل تلك البوتات على قواعد مُعيّنة عن طريق الأشخاص، من خلال أوامر مُحدّدة مسبقًا يمكن للشخص الاختيار فيما بينها.
- ويمكن لبوتات المُحادثة أن تصل إلى مستوى من الاستقلال الفكريّ، خاصّة أنّ لديها ميزة التّعلّم من المُدخلات البشريّة، وكذلك ميزة البحث عن الكلمات المفتاحيّة.
- يُستخدم الذّكاء الاصطناعيّ في بوتات المُحادثة، لذا فهي مبنية على أوامر مُستقلّة فكريًا، كما يُمكنها الذّكاء الاصطناعيّ من مُعالجة اللّغة لجعلها أشبه باللّغة الطّبيعيّة للبشر.

ما فائدة روبوتات الشبكة العالمية؟

- السرعة الكبيرة؛ فهي أسرع من البشر خاصّة في المهامّ المُتكرّرة والنمطيّة.
- توفير الوقت والتّكاليف وكثيرًا من الخيارات للشّركات والعملاء.
- مُتاحة على مدار اليوم.
- يمكنها أن تساعد الشّركات الكبيرة في التّواصل مع أعداد أكبر من الجمهور دون مشكّلة.
- يمكن تخصيصها.
- تُستخدم في مُختلف الأغراض.
- يمكنها أن تُحسّن من تجربة المُستخدم.

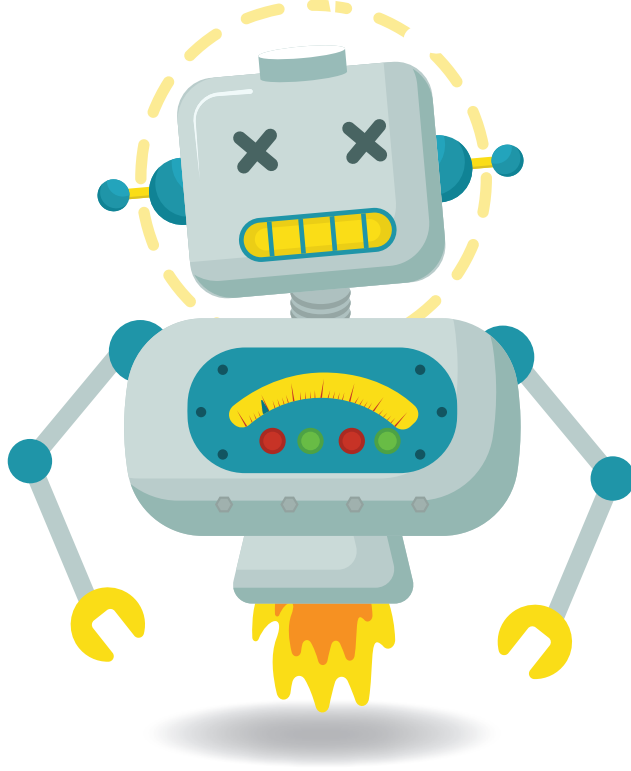
كيف تحمي جهازك من البوتات الضارة؟

- تثبيت البرامج المُتخصصة في مكافحة البرمجيات الضارة؛ لأنها تحجب الفيروسات والمُخترقين وأي برمجيات ضارة يمكن أن تُصيب أجهزتك.
- التحديث المستمر للبرامج والأنظمة التي تستخدمها.
- استخدام كلمات مرور قوية يُصعب تخمينها.
- تجنب الضغط على الروابط المجهولة، سواء التي تجدها بالمصادفة أم التي تصلك في رسالة أم حتى عبر البريد الإلكتروني.
- تجنب المواقع الإلكترونية، خاصة تلك التي تستخدم الإعلانات المنبثقة أو التي تظهر لتُخجب أغلب المحتوى، والتي تدّعي أنها يمكنها الكشف عن الفيروسات أو حماية أجهزتك.
- تفعيل الجدار الناري الذي يساعد في حجب الهجمات الخبيثة.
- استخدام برنامج تحليل السلوك وإدارة البوتات المُتخصص في إيقاف البوتات الضارة.

عندما يتعرض جهازك للإصابة بالبوتات عليك أن تفعل التالي:

1. افصل جهازك عن الإنترنت فوراً لكي تُوقف سرقة البيانات والمعلومات، ومنع دخول البوتات إلى الشبكة.
2. انقل كل البيانات المهمة إلى جهاز آخر أو قرص صلب خارجي بعد التأكد من أنه خالٍ من البرمجيات الضارة.

3. قُم بإعادة ضبط الجهاز إلى وضع المصنع، وستتخلص هذه الخطوة من البوتات، ولكن للأسف ستفقد معها كل الأشياء الأخرى على الجهاز ولكن يمكن استرجاع البيانات من النسخة التي تم إنشاؤها في الخطوة السابقة..
4. أخيراً نظّف الحاسوب واستخدم أدوات الأمان اللازمة.



الحقيبة التدريبية الثامنة



سياسة أمان المحتوى

الفصل الأول: مفهوم سياسة أمان المحتوى (CSP) وآلية عملها
الفصل الثاني: كيفية تفعيل سياسة أمان المحتوى (CSP)
والمخاطر الرقمية التي تحد منها

الفصل الأول: مفهوم سياسة أمان المحتوى (CSP) وآلية عملها

مفهوم سياسة أمان المحتوى (CSP)

سياسة أمان المحتوى هي العنصر الأساسي المسؤول عن تقديم معايير الأمان الخاصة بالحاسوب أو الأجهزة المشابهة، من خلال منع البرمجيات الضارة عبر المواقع التي تستخدم XSS أو هجمات القرصنة أو هجمات إدخال التعليمات البرمجية الأخرى الناتجة عن تنفيذ محتوى ضار في سياق صفحة الويب الموثوقة، كما أنها طريقة لتقليل مخاطر مختلف أنواع الهجمات وإزالتها تمامًا من خلال تحديد مصادر موثوقة لمحتوى صفحات الويب.

آلية عمل سياسة أمان المحتوى (CSP)

يسمح معيار CSP لمسؤولي الويب بإرسال محتوى الويب عبر HTTP/HTTPS أو عنوان الاستجابة، مع تحديد المصادر التي يُسمح للمتصفح بتحميل المحتوى الخاص بها، أو منها، وبالطبع لا يتم تحميل المحتوى من أي مصادر غير مذكورة صراحة في CSP وكذلك لا يتم تشغيلها على المتصفح، ويتضمن هذا كل أنواع المحتوى، سواء النصوص، الأنماط، الصور، الوسائط، الإطارات، والخطوط.

تعد سياسة أمان المحتوى مهمة لأنها تعمل كطبقة حماية إضافية يمكنها التخفيف من تأثير الثغرات الأمنية الأخرى في تطبيقات الويب، ولكنها لا تحل محل ممارسات الترميز الجيدة أو تدابير الأمان الأخرى، فهي فقط طبقة إضافية من الدفاع.





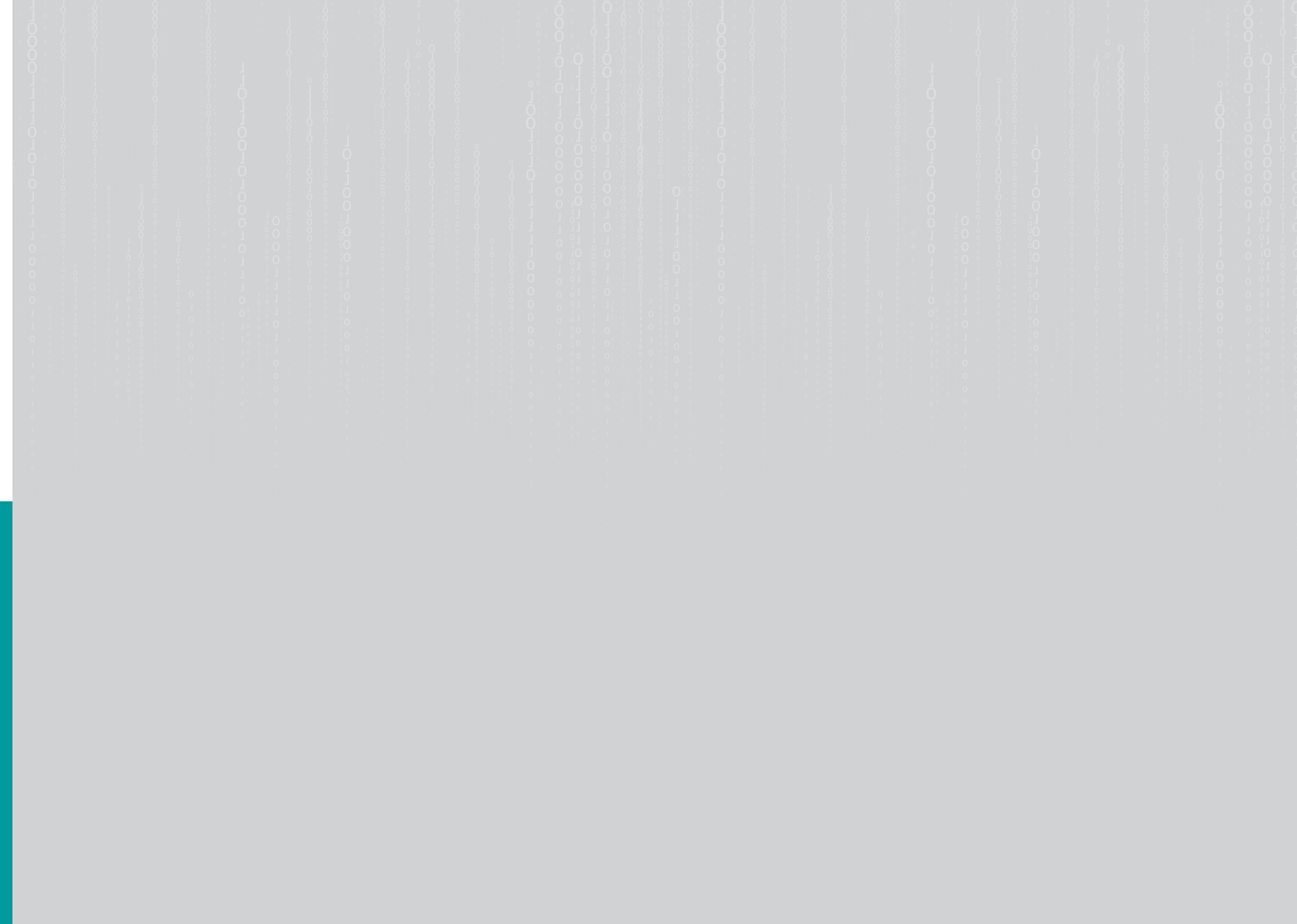
الفصل الثاني: كيفية تفعيل سياسة أمان المحتوى (CSP) والمخاطر الرقمية التي تحد منها

كيفية تفعيل سياسة أمان المحتوى (CSP)

يتم تفعيل سياسة أمان المحتوى عن طريق الإعدادات الخاصة بالمواقع، ثمّ الدّخول إلى إعدادات الخصوصية وإعدادات الأمان بالمُتصفح الخاصّ بتصفّح الإنترنت وبعدها تغيير إعدادات السّماح لسياسة أمان المحتوى، كذلك تفعيل إمكانية إرسال التقارير الأمنية التي تُنتجها هذه الميزة الرائعة.

المخاطر الرقمية التي تحد منها سياسة أمان المحتوى (CSP)

- Default Source
هو العامل الرئيس لتوجيهات الجلب الأخرى عندما لا يتم تحديدها صراحة.
 - Child-Source
يسرد المصادر الموثوقة للقائمين على الويب وسياقات التصفح المتداخلة التي تمت.
 - Script-Source
يحدد المصادر الموثوقة لـ Java Scripts.
 - Object-Source
يحدد المصادر الموثوقة لعناصر: <Object> و <Embed> و <Applet>.
 - Style-Source
يحدد المصادر الموثوقة لأنماط عرض المحتوى (CSS).
 - Img-Source
يحدد المصادر الموثوقة للصور والأشكال المفضلة.
- Frame-Source
يحدد المصادر الموثوقة لسياقات التصفح المتداخلة التي يتم تحميلها باستخدام عناصر مثل <Frame> و <Iframe>
 - Connect-Source
يحدد من عناوين URL التي يمكن تحميلها باستخدام واجهات البرنامج النصي.
 - Upgrade-Insecure-Requests
يوجه متصفح الويب للتعامل مع جميع عناوين URL غير الآمنة الخاصة بالموقع، وتلك التي يتم عرضها عبر HTTP كما لو تم استبدالها بعناوين URL آمنة.
 - Require-sri-for
يتطلب استخدام Subresource Integrity (SRI) للنصوص أو الأنماط الخارجية على الصفحة.





الحقيبة التدريبية الخاصة
بأولياء الأمور

حماية الأجهزة الإلكترونية ومواجهة الاختراقات الأمنية
الفصل الأول: أهمية أمن الأجهزة الإلكترونية والشبكات
الفصل الثاني: أنواع المخاطر الرقمية التي تواجه الأجهزة
الفصل الثالث: كيفية حماية الأجهزة من الأخطار الرقمية

الفصل الأول: أهمية أمن الأجهزة الإلكترونية والشبكات

الحفاظ على أمن وسريّة المعلومات أمر شديد الأهمية، ولا يمكن الوصول إليه إلا بحماية الأجهزة الإلكترونية والشبكات من الاختراقات الأمنية والاختراقات في قواعد البيانات، ويمكن أن يتّج عن هذه الاختراقات مشكلات كبيرة، خاصّة لدى الشركات التي تتعامل مع بيانات العملاء السريّة والتي يمكن أن تُهدّد أمن العملاء، وبالتالي تُصبح هذه الشركات في خطر الوقوع في قضايا كثيرة بسبب تسرّب البيانات، وكذلك خطر ضياع سُمعتها وخسارتها للعملاء.

أهمية الاستقرار الرقمي للشبكات والأجهزة المتصلة بها

الاستقرار الرقمي من أهم الأمور التي يجب أن تحرص الشركات وحتى الأفراد على حمايتها؛ لأنّ تهديد هذا الاستقرار يعني مخاطرة كبيرة تتعلّق بـ:

- **المعلومات؛** خاصّة أنّ الأمان الرقمي يعني حماية بياناتك ومعلوماتك الشخصية الخاصّة بالدخول إلى نظام العمل، نظام المدرسة، أو أي نظام آخر، أو التي تستخدمها لإنجاز المهام المهمّة أو البيانات الخاصّة بالملفّات النهائيّة لتلك المهام.
- **الاستقرار في العمل؛** لأنّه عقب التّعرّض لأيّ هجوم إلكترونيّ تحتاج المؤسسات والشركات إلى وقتٍ كبيرٍ للتّعافي والعودة إلى الاستقرار ما قبل التّعرّض للهجوم، وبالتالي الجفاف على الأمان والاستقرار الرقميّ يضمن استمرار العمل واستقراره.
- **تجنّب المشكلات القانونيّة؛** لأنّ تسريب البيانات الخاصّة بالأفراد أو الشركات سيُعرّضك للمساءلة القانونيّة وقد تُعاقب لهذا السّبب.





المخاطر الرقمية التي تواجه الأجهزة الرقمية (الهواتف، الأجهزة اللوحية، الحواسيب)

- استغلال الثغرات الأمنية التي تستهدف ثغرات النظام أو الثغرات المرتبطة بالتطبيقات المستخدمة -مثل أنظمة التشغيل غير المحدثة أو القديمة أو غير المدعومة-، التي تصبح الأكثر عرضة للهجمات، لما فيها من ثغرات يمكن استغلالها بسهولة.
- خرق كلمات المرور الضعيفة أو التي يسهل تخمينها.
- هجمات نشر البرمجيات الضارة.
- الهندسة الاجتماعية، التي تساعد المخترقين على خداع الضحايا وخرق أجهزتهم بسهولة، فقط بمراقبة وتحليل سلوك الضحية المحتملة والعمل على إيقاعه.

الفصل الثاني: أنواع المخاطر الرقمية التي تواجه الأجهزة

هجوم الفدية

هذا الهجوم يعتمد على إرسال ملف مُرفقات أو الضّغط على رابط ليقوم تلقائيًا بتحميل برنامج ضار على الجهاز ثم يختفي هذا البرنامج بسهولة، وفي وقت مُحدد تمّ ضبطه مسبقًا يتعطّل الجهاز كليًا، لتصلك رسالة تطلب منك دفع فدية مقابل استرجاع البيانات والتحكم في الجهاز.

سرقة بيانات الأجهزة

سرقة البيانات تتم بعددٍ من الطرق، منها البرمجيات الخبيثة والديدان والفيروسات وبرمجيات أحصنة طروادة، وكلها تستهدف الأجهزة للحصول على البيانات والمعلومات المسجلة عليها أو التحكم بها، أو ربما تعطيلها أو إتلافها أو تدميرها.

الوصول غير القانوني وغير المصرح به

يستخدم المخترقون أكثر من شكلٍ من أجل الوصول إلى البيانات والمعلومات التي لا يُسمح لهم بالوصول إليها، ويُعدّ الاحتيال عبر الإنترنت والتصيد الاحتياليّ من أبرز وأشهر الأشكال التي يستخدمها هؤلاء للوصول إلى البيانات والسيطرة على الأجهزة والشبكات.

البرمجيات الضارة

من أبرز أشكال البرمجيات الضارة التي تُستخدم لاختراق الأجهزة والشبكات:

- الفيروسات.
- الديدان الفيروسية.
- أحصنة طروادة.
- برمجيات التجسس والمتابعة.

الفصل الثالث: كيفية حماية الأجهزة من الأخطار الرقمية

كيف تحمي نفسك من الاختراقات الأمنية؟

- استخدم كلمات مرور قوية وقم بتفعيل المصادقة الثنائية أو متعددة العوامل كلما أمكن ذلك.
- استخدم كلمة مرور مختلفة في كل حساب من حساباتك.
- أغلق الحسابات التي توقفت عن استخدامها.
- احرص على تغيير كلمات المرور من وقت لآخر بانتظام (المدة المقترحة من شهرين إلى ثلاثة أشهر).
- قبل أن تتخلص من أجهزتك الإلكترونية؛ تأكد من مسح كافة البيانات والحسابات الموجودة عليها.
- اصنع نسخة احتياطية من ملفاتك المهمة.
- آمن هاتفك باستخدام قفل الشاشة.
- استخدم برامج الحماية والجدران النارية.
- ركز جيدًا قبل النقر على أي رابط.
- تأكد من صيغة الروابط التي تدخل عليها ومن استخدام بروتوكول Http.
- راجع حساباتك البنكية وتقاريرك الائتمانية باستمرار للتأكد من عدم وجود حركات غير طبيعية.

- اغرف قيمة بياناتك ولا تُفصح عنها لأي شخص أو من خلال منصات التواصل الاجتماعي.



المحور الخامس

الألعاب التدريبية التفاعلية

في إطار مشروع الزيارات الميدانية للمدارس؛ سيتم تقديم عدّة ألعاب تدريبية للطلبة، والتي تُحقق عدّة أهداف، منها تقديم معلومات ذات صلة بمفاهيم الأمن السيبراني والسلامة الرقمية للطلبة في إطار من التسلية والترفيه والتنافس، فهذه الألعاب تُعدّ رديفًا وداعمًا للمادة العلمية التي سيتم تقديمها للطلبة ضمن الحقائق التدريبية.

وبشكلٍ عامّ، تُعدّ الألعاب التدريبية أداةً فعّالة في تعليم الأطفال والياfeعين أساسيات الأمن الرقمي ومبادئ السلامة الرقمية.

وتستمدّ هذه الألعاب فاعليتها من كونها تُضمن جذب انتباه وتركيز الطلبة؛ نظرًا لاعتمادها على عنصر التشويق والترفيه، فالطالب يحصل على المعلومة من خلال إطارٍ ترفيهيٍّ؛ وهو ما يحول دون الشعور بالملل أو الرتابة.

يبلغ عدد الألعاب التدريبية خمس ألعاب، وهي تُغطّي مختلف المراحل التعليمية، فمنها ما هو مُوجّه لطلبة المرحلة الابتدائية وأخرى للإعدادية والثانوية، وهي في مجملها ألعاب تفاعلية، بمعنى أنها تتطلب مشاركة أكثر من طالب في اللعبة، وفيما يلي تبيان مُختصر لهذه الألعاب.

اللُّعْبَةُ الْأُولَى

لُّعْبَةُ Cyber Block

العُمر المُخَصَّص لِلُّعْبَةِ

10+ سنوات

فكرة اللُّعْبَةِ

"ساير بلوك" هي لُّعْبَةُ تُقَدِّمُ أَفْكَارًا وَمَعَارِفَ أُسَاسِيَّةً مُرْتَبِطَةً بِالْأَمْنِ السَّيْبِرَانِيِّ، وَمَا يَتَعَلَّقُ بِهِ مِنْ مَوْضُوعَاتٍ مُهِمَّةٍ بِشَكْلِ مُبَسَّطٍ وَمُسَلِّ لِلطَّلَبَةِ وَالتَّيَافِعِينَ؛ بِمَا يَسَاعِدُ الطَّلَبَةَ عَلَى التَّعَلُّمِ بِطَرِيقَةٍ مُبْتَكِرَةٍ وَغَيْرِ تَقْلِيدِيَّةٍ.



تقوم اللُّعْبَةُ فِي جَوْهَرِهَا عَلَى تَقْدِيمِ مَعْلُومَاتٍ لِلطَّلَبَةِ حَوْلَ مَفَاهِيمِ ذاتِ صِلَةٍ بِالْأَمْنِ السَّيْبِرَانِيِّ وَالسَّلَامَةِ الرَّقْمِيَّةِ، كَمَفَاهِيمِ أَمْنِ الشَّبَكَاتِ وَأَمْنِ المَعْلُومَاتِ وَالتَّطبيقاتِ وَغَيْرِهَا مِنَ المَفَاهِيمِ؛ بَحِثُ تُقَسِّمُ المَفَاهِيمَ إِلَى مَفَاهِيمٍ إيجابية كَالسَّرِّيَّةِ وَالسَّلَامَةِ وَغَيْرِهَا، وَمَفَاهِيمٍ سَلْبِيَّةٍ كَالجَرَائِمِ الإِلِكْتروْنِيَّةِ وَسَرَقَةِ البَياناتِ، وَغَيْرِهَا.

كُلُّ هَذِهِ المَفَاهِيمِ، الإيجابية والسلبية، مطبوعة على لَوْحِ اللَّعْبِ، وَالْمَفَاهِيمُ الإيجابية تُسَمَّى بِالمناطق الآمنة، بينما السلبية تُسَمَّى بِالمناطق غير الآمنة؛ وَلِكُلِّ طَالِبِ مُجَسِّمٍ خَاصٌّ بِهِ يَتَحَرَّكُ بِهِ عَلَى هَذَا اللَّوْحِ، وَفِي حَالِ جَاءِ مُجَسِّمِهِ عَلَى مَنطِقَةِ آمنة عَلَى اللَّوْحِ يُعْطَى بِطَاقَةِ جَائِزَةٍ فِيهَا نَقَاطٌ. أَمَّا فِي حَالِ جَاءِ مُجَسِّمِهِ عَلَى مَنطِقَةِ غير آمنة عَلَى اللَّوْحِ فَيُعْطَى بِطَاقَةِ عَقُوبَةٍ قَدْ تَحْرَمُهُ مِنَ اللَّعْبِ أَوْ تُخْصِرُهُ بَعْضَ النُّقَاطِ.

الفريق الفائز هو الحاصل على أكبر عددٍ من النُّقَاطِ.

اللّعبة الثانية

Cyber Quiz

العمر المخصّص للعبة

7+ سنوات

فكرة اللعبة

اللعبة تأخذ الطالبة الصغار في جولة تنافسية شيقة، من خلال توجيه الأسئلة والإجابة عنها في موضوعات مبسطة وسلسة ذات صلة بالأمن السيبراني خلال توقيت زمني محدد، كل هذا في قالب تنافسي جذاب يضمن الترفيه والتعلم بطريقة مبتكرة.

تتألف اللعبة من 25 بطاقة، تهتم كل بطاقة بمفهوم من مفاهيم الأمن السيبراني والسلامة الرقمية، مثل سلامة البيانات والجرائم الإلكترونية، وغيرها من المفاهيم، وكل بطاقة مرتبطة بأربعة أسئلة، فيكون عدد الأسئلة الإجمالي 100 سؤال.

تتألف اللعبة أيضًا من 25 مجسمًا مرقّمًا من 1 - 25؛ وفي بداية اللعبة يقوم كل طالب باختيار مجسم من المجسمات، ويحصل الطالب على بطاقة اللعب التي رقمها يماثل رقم المجسم الذي اختاره، وهنا عليه أن يجيب عن أحد الأسئلة الأربعة المرتبطة بالبطاقة.

في حال أجاب الطالب إجابة صحيحة فإنه سيحصل على نقطة، وهي على شكل Coins، كل Coins يُعادل نقطة واحدة، والطالب الفائز هو الذي يحصل على أعلى عدد من النقاط في نهاية اللعبة.



اللّعبة الثالثة

سيبرونو Cyberno

العمر المُخصَّص للعبة

17+ سنة

فكرة اللعبة

الفكرة الأساسية من لعبة «سيبرونو» هي توعية طلبة المرحلة الثانوية بمُصطلحات ومفاهيم الأمن السيبراني، وكذلك مخاطر وتهديدات الأمن السيبراني بطريقة أكثر فُدرّة على تحفيز التفكير والرّبط بين المعلومات السيبرانية. وتُسهم في اكتساب المعلومات وفُق آليّة تنافسيّة مُبتكرة. واللعبة تشاركيّة جماعيّة ما يُضفي جَوًّا تنافسيًّا حماسيًّا.

تتألّف اللعبة من 116 بطاقة، ذات صلة بمفاهيم الأمن السيبراني والسلامة الرّقميّة. في بداية اللعبة يُوزّع على كلّ طالب 7 بطاقات، ثمّ يقوم كلّ طالب بقراءة مُحتوى إحدى بطاقاته على طالب آخر؛ بحيث عليه أن يُخمن عنوان البطاقة التي يقرأ الطالب الأوّل معلّوماتها، وفي حال نجح في التّخمين، فإنّه سيتمكّن من التّخلص من إحدى بطاقاته، والطالب الفائز هو أوّل من يتمكّن من التّخلص من كلّ بطاقاته.

وللمزيد من الحماس، تُوجد بطاقات خاصّة تَمنح حاملها مِيزَات إضافيّة تسمّح له بالتّحايّل على الإجابة أو تغيير السؤال.



اللُّعْبَةُ الرَّابِعَةُ

سَايِر واي Cyber Way

العُمر المُخصَّص للُّعْبَةِ

15+ سنة

فكرة اللُّعْبَةِ

تأتي فكرة اللُّعْبَةِ من خلال إجراء مُسابقات معرفيَّة حول الأمن السيبراني بين الطُّلَبَةِ، تجمع اللُّعْبَةِ بين التَّحدِّي والمُنَافَسة والمَعْرِفَة والتَّسْلِيَة، فهي تُقدِّم معلومَاتٍ، وتختبر المَعْرِفَة للطُّلَبَةِ ضمن إطار تنافسي قائم على المُنَافَسة والتَّسْلِيَة.

يُقسَّم الطُّلَبَةُ إلى ثلاث فِرَق في اللُّعْبَةِ؛ طَالِب واحد على الأقل في كلِّ فريق، ولكلِّ فريق لون مُختلف، أحمر وأزرق وأرجواني، ولهذه الألوان دلالاتها الخاصَّة في الأمن السيبراني.

كما تتألَّف اللُّعْبَةُ من لوح لعب، مُقسَّم إلى مُربَّعات مُرقَّمة من 1 - 100، والمُربَّعات مُلوَّنة بألوان الفِرَق، ولكلِّ فريق مُجسَّم خاص به يتحرَّك به على لوح اللعب، وحَجَر نرد يرميه الطُّلَبَةُ، ويحدِّد عدد المُربَّعات التي سينتقل بها مُجسَّم الطَّالِب على لوح اللعب.

وتتألَّف اللُّعْبَةُ من عددٍ من البطاقات، لكلِّ فريق بطاقاته الخاصَّة به، بحيث يسأل كلُّ فريق أحد الفِرَق الأخرى سؤالًا، وفي حال تمكَّن الفريق الآخر من الإجابة يقوم بنقل مُجسَّمه مربعًا إلى الأمام.

ولزيادة الحماس في اللُّعْبَةِ، يوجد على لوح اللعب رُموز بعضها سلبي وآخر إيجابي؛ بحيث تمنح الفريق الذي يكون مُجسَّمه على هذه الرُّموز مَيَزَة التَّقدُّم للأمام، أو تُعاقبه بالرجوع للخلف.

والفريق الفائز هو مَنْ يصل بدايةً للمربع رقم 100.



اللّعبة الخامسة

بطاقات الأفكار التّعليميّة

العمر المُخصّص للّعبة
4-6 سنوات (المرحلة الابتدائيّة)

فكرة اللّعبة

لّعبة توعويّة تعليميّة للطلّبة الصّغار تستخدم طريقة الألوان والرّسوم والتّلوين، وتهدف إلى تعريفهم برّموز المفاهيم العامّة ذات الصّلة بالأمن السيبرانيّ والسّلامة الرّقميّة، عبر خطواتٍ بسيطةٍ يسهّل استيعابها خلال هذه السنّ 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.



المحور السادس

**الدَّورُ الْمُتَوَقَّعُ مِنْ
أَوْلِيَاءِ الْأُمُورِ فِي
مَشْرُوعِ سَايْبِرِ إِيكُو**

يُعدّ تعاؤن أولياء الأمور مع الفريق التنفيذي لمشروع الزيارات الميدانية مدخلًا رئيسًا لنجاح المشروع وتحقيق أهدافه، ولذلك لا بُدّ من تحديد الأدوار المتوقعة من أولياء الأمور في سياق المشروع، وتوضيح آليات ومراكز هذا التعاؤن.

الفرق بين الأنشطة الصفية واللاصفية

تتضمن الأدوات المستخدمة في سياق مشروع الزيارات الميدانية تنفيذ نوعين من الأنشطة التدريبية، وهي التدريب الصفّي واللاصفّي، ولا بُدّ لأولياء الأمور من الوعي التام بهذه المفاهيم.

- **الأنشطة الصفية:** هي تلك الأنشطة التي يمارسها الطالب داخل الصف بمشاركة المُدرّب أو المُعلّم وتحت إشرافه، من أجل تحقيق الأهداف التدريبية التي يهدف إليها المشروع.
- **الأنشطة اللاصفية:** وهي الأنشطة التي يمارسها الطالب خارج إطار الصف، والتي تهدف إلى استمرار العمل التوعويّ في منزل الطالب وبإشراف غير مُباشر من ذويه، ولا بأس أن يُشارك أولياء الأمور معهم في هذه الأنشطة.

توفير الوسائط الثقافية والتعليمية

حرص مشروع سايبّر إيكو على توفير أنواع مُتعدّدة من الوسائط الثقافية للطلّبة والمُتدربين من أجل مساعدة الطّلبة على الفهم واستيعاب المحتوى التدريبيّ

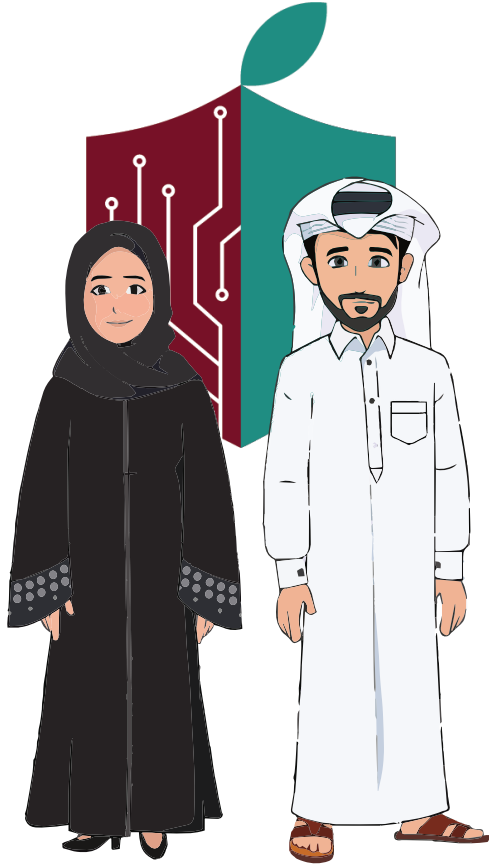
المُقدّم لهم، وبالطبع تمّ وُضع وسائط ثقافية مُناسبة لكلّ مرحلة من مراحل الطّلبة المُشاركين وتتناسب مع الموضوعات التي يدرسونها لكي تساعد على إتقان المحتوى وفهمه بشكلٍ أعمق وأقرب إلى الواقع.

التواصل المستمر مع المُعلّمين

من الضّرورات التي تضمن نجاح هذا المشروع ضرورة التواصل بين المُعلّمين وأولياء أمور الطّلبة؛ وذلك لأنّه لا بُدّ من إيجاد تكامل بين دور المُدرّب أو المُعلّم في الصف ووليّ الأمر في المنزل، فكلّهما مَعْنِيّ بمصلحة الطّفل، والهدف الأساسي والأهمّ لهما هو إنجاح المشروع وتعزيز التحصيل الرّقميّ للطلّبة وزيادة قُدْرَتهم على التّعامل الآمن مع التّكنولوجيا.

معالجة المشكلات

يُوفّر مشروع سايبّر إيكو كافّة الإمكانيات التي تضمن النّجاح وتحقيق أهداف المشروع، ولكن وقوع المشكلات أمر وارد بالطبع ولذلك تمّ توفير العديد من وسائل الاتّصال المُباشر مع إدارة البرنامج وكذلك مع القائمين عليه ومع المُعلّمين وأولياء الأمور من أجل التّصرّف الفوريّ والسّريع حيال أيّ مشكلة قد تطرأ أو قد تؤثر في الطّلبة ومستوى تحصيلهم للمحتوى الخاصّ بالمشروع.



الدور المتوقع من أولياء الأمور

- على الوالدين أن يُقدِّما الدَّعم الكافي لأبنائهم في فهم واستيعاب محتوى الورش التدريبية، والتَّأكُّد من تلقِّيهم المعلومات بطَرَح الأسئلة المختلفة عن الموضوع، وتقييم إجاباتهم، ومُساعدتهم في البَحْث والاطِّلاع الخارجي، وتوسيع إطار الاستكشاف المعرفي.
- على الوالدين أن يَهْتَمَّا بتخصيص وقتٍ كافٍ لمُشاركة أبنائهم الألعاب التفاعلية المختلفة في أوقات فراغهم، وقراءة دليل الألعاب جيِّدًا؛ لضمان تحقيق المُتعة وتحقيق أقصى استفادة من اللعبة للطَّرفين في الوقت ذاته.
- على الوالدين التَّواصل المُستمر مع المُعلِّم في شأن محتوى الورش التدريبية، والتَّأكُّد من فهم الموضوعات المُتعلِّقة بها، والاستفسار من المُعلِّم عن أيِّ معلومات قد يَضُغِب عليهم استيعابها؛ بما يساعدهم على دَّعم أبنائهم والتَّأكُّد من فهمهم التَّام للمحتوى.



تكامُل دَورِ أَوْلِيَاءِ الأُمُورِ معَ دَورِ المُعَلِّمِينَ

العلاقة بين وليّ الأمر والمُعَلِّم من الرُّكائز الأساسيّة لأيّ نظامٍ تربويٍّ وتربويٍّ كاملٍ وناجحٍ، وبالتالي لا بُدَّ أن يكون هناك تواصل مستمرٌّ وصيغة مُرضية للتفاعل بين وليّ الأمر والمُعَلِّم، وفيما يلي أهمُّ المُرتكزات التي تُنظِّم صيغَ التَّعاون بين المُعَلِّمين وأَوْلِيَاءِ الأُمُور في إطار مشروع سايبر إيكو:

- **إطار التَّعاون في مجال التَّمارين اللَّاصقيّة:** قد يحتاج الطَّلَبَة إلى بعض الاستفسارات حول التَّمارين اللَّاصقيّة التي سيُكلِّفون بها في سياق مشروع الرِّبازات المبدائيّة، وبعض هذه الاستفسارات قد لا يتمكّن أَوْلِيَاءِ الأُمُور من تقديم إجابات عنها، لذلك قد ينقل أَوْلِيَاءِ الأُمُور هذه الاستفسارات لمُعَلِّمي الصَّف الذين سيُقدِّمون إجابات عنها، أو ينقلونها بدورهم إلى الفريق التَّنفذيّ على المشروع.
- **التَّقييم:** عمليّة تقييم استفادة الطَّلَبَة من المحتوى التَّربويّ ستتمّ بالتَّعاون بين المُعَلِّمين وأَوْلِيَاءِ الأُمُور معًا، من خلال تبادل المعلومات حول تطوُّر سلوك الطَّالب في التَّعامل مع الإنترنت ومع الأدوات التَّكنولوجيّة.

