دليل تدريبي لمرشدي/ات و معلمي/ات المدارس

لرفع وعي الطلاب والطالبات حول الأمان الإلكتروني والحماية من التحرش والابتزاز على الإنترنت

إعداد تنمية وإعلام المرأة/ تام

فريق الاعداد:

مها الزغاري

إبراهيم سليم

اشراف :

سهير فراج

تدقيق و مراجعة :

صبحي الخطيب

2020

الفهرس

- **القسم الأول: دليل الفئة العمرية من 11–16 عامًا**
  - **مقدمة**
  - **مفهوم وأهمية الخصوصية الرقمية**
  - **الأمان الرقمي للوقاية من العنف الإلكتروني**
  - **المواقف التي تستدعي المساعدة وآليات الإبلاغ**
  - **مساعدة الآخرين**
  - **العنف والابتزاز الإلكتروني**

- **القسم الثاني : دليل الفئة العرية من 6–10 عامًا**
  - **مقدمة**
  - **لا تتحدث مع الغرباء– الحفاظ على المعلومات الشخصية**
  - **المواقف التي تستدعي طلب المساعدة**
  - **أهمية الإيجابية واللطافة عبر الإنترنت**
  - **وقت الشاشة والتوازن الصحي**
  - **اللعب عبر الإنترنت**
  - **الإعلانات**
  - **اليوتيوب**
  - **بدائل ومكملات للإنترنت**

القسم الأول : الفئة العمرية من 11-16 عامًا

مقدمة

يسعى هذا الجزء من الدليل للنهوض بتوعية الطلاب والطالبات من جيل 11 عاماً حتى جيل 16 عاماً عن موضوع الأمان الإلكتروني، وحمايتهم/نّ من التحرش والابتزاز على الشبكة.

كما هو معلوم فإنّ التطورات التكنولوجية دائمة التغيير، لذا فقد اعتمد هذا الدليل على فعاليات عامة تتطرق للتوجه والتفكير الحذِر الذي نودّ للطالب/ة أن يطوره، وعندما يتطور هذا الفهم العام، تصبح المنصّات المختلفة الحالية والمستقبلية أقلّ أهمية؛ لأنّ الطالب/ة يكون قد طوّر التفكير النقدي والحذِر تجاه المنطق الذي سيحميه.

كل الأنشطة المذكورة أدناه تمت تجربتها، وتم تطوير بعضها على يد مختصّين/ات في مجال التوعية الرقمية، وعلى الرغم من تحديد الفئات العمرية للأنشطة إلّا أنه يمكن تمرير بعض الأنشطة لأجيال غير المذكورة، مع الأخذ بعين الاعتبار ملاءمة الفعالية للجيل.

ملاحظة للمدرب/ة:

-قد يشعر بعض الطلاب والطالبات بالخوف، أو قد يقررون العزوف عن استخدام الإنترنت، عليك التأكيد أن الهدف هو الحذر والانتباه، وليس الخوف أو العزوف عن الإنترنت.

-تفسد المعلومات بشأن الأمن الرقمي والحماية مع الوقت، لذا يجب التنبه لذلك وذكره.

التعرف على مفهوم وأهمية الخصوصية الرقمية

مفهوم الخصوصية الرقمية:

من المهم أن يتَحَكُّم الأفراد في مدى وتوقيت وظروف مشاركة حياتهم مع الآخرين، وتدخل الخصوصية كحقّ يمارسه الفرد للحدّ من اطلاع الآخرين على مظاهر حياته، والتي يمكن أن تكون أفكاراً أو بيانات شخصية.

لماذا تعتبر الخصوصية الرقمية مهمة؟

سهّل الإنترنت التواصل مع العائلة والأصدقاء والأشخاص الذين يتشاركون معنا اهتماماتنا، فعلى الدوام نرسل رسائل ونشارك صوراً ونحدّد مواقع تواجدنا، وننضم إلى محادثات على وسائل التواصل الاجتماعي، ونشارك ونعلّق على منشورات دون التفكير أحياناً في الأشخاص الآخرين الذين يمكنهم رؤيتنا، وقد تصل الصورة أو المشاركة التي أرسلناها إلى أشخاص لم نعتقد أنهم سيرونها، سواءَ الآن أو لاحقاً، وعند نشر شيء على الإنترنت من الصعب حذفه. لذا عليك الانتباه دوماً للأمور التالية:

- يمكن رؤية معلوماتك على الإنترنت من قبل أشخاص لم تلتقِ بهم مطلقاً.
- عند نشر شيء عنك أو من قبلك على الإنترنت قد يبقى عليه للأبد، حيث لا يمكنك محو ما نشرته حتى لو أدركت لاحقًا أنّك لم تقصده أو لا تريده.

هذا ما يجعل من الخصوصية موضوعا أساسياً ومهماً، ويمكنك حمايتها من خلال عدم مشاركة إلّا ما ترغب فعلاً بمشاركته، واختيار ما تريد نشره أو مشاركته على الإنترنت بحذر.

جميع المعلومات المتوفرة عنك على الإنترنت والتي تشمل الصور والفيديوهات والمنشورات وتعليقاتك، وغيرها الكثير من الآثار التي تتركها عند استخدام الإنترنت تمثل "حضورك الرقمي" أو ما يُعرف باسم "البصمة الرقمية"، وإنّ المحافظة على حضور إيجابي على الإنترنت لا يقل أهمية عن الحفاظ عليه في العالم الحقيقي، مثل المدرسة والمجتمع والعائلة.

من المهم معرفة الحالات التي لا ينبغي فيها نشر مشاركة أحد، أو الرد على مشاركة شخص ما، أو التعليق على صورته أو منشوره أو مشاركة معلومات خاطئة، لقد سمعنا جميعنا جملة "فكر قبل النشر!"، وهي بلا شك نصيحة جيدة؛ حيث إن الوسيلة المثلى لاحترام خصوصيتك وخصوصية الآخرين هي التفكير في ما هو مناسب للنشر، ومن قد يرى مشاركتك، وما هو التأثير المحتمل عليك وعلى الآخرين، ومتى يجب عدم النشر على الإطلاق.

قد تكون مشاركة بياناتك مفيدة وممتعة لك، وغالباً ما يكون من الضروري مشاركتها للتفاعل مع الأشخاص الآخرين في الوقت الحالي. لكن هذا لا يخلو من المخاطر؛ فبياناتك الشخصية يمكن أن تكشف الكثير عنك وعن أفكارك وحياتك، ومن السهل استغلال هذه البيانات لإيذائك، لذا عليك التنبه جيدًا...

فكر مليّا في الرسائل والصور التي تتقاسمها– حتى مع الأصدقاء– وإذا كنت تخشى أن يقرأها أو يراها شخص ما، فلا تنشرها.

ثق بحدْسك! فإذا شعرت بعدم الارتياح للتحدث إلى شخص ما، فلا تردّ عليه ولا تُعِر الاهتمام بما يرسل، وتوخى الحذر من فتح أي روابط يرسلها لك.

النشاط 1	**ماذا يخبر عنك الإنترنت؟**
الفئة العمرية	14 –16 عامًا
الهدف	تعزيز توجهات الطلاب/الطالبات حول كميّة وطبيعة المعلومات التي يشاركونها على الإنترنت، وتأثير ذلك على الخصوصية.
الطريقة	عمل مجموعات، وإجراء المناقشات
الأدوات اللازمة	أوراق، أقلام، لوح
التفاصيل	– يقسّمُ/تُقسّم المدربُ/ة الطلاب/الطالبات لمجموعات صغيرة: يطلب/تطلب المدرب/ة منهم كتابة نوعية المعلومات التي يشاركونها على موقع فيسبوك أو انستغرام على ورقة مثل: (صور شخصية، آراءهم/نّ، أماكن تواجدهم/نّ، بياناتهم/نّ، الاسم، تاريخ الميلاد، البريد الإلكتروني، رقم الهاتف، اسم المدرسة، المغني المفضل، إلخ...) – ثم يقوم الطلاب/ات بعرض النتائج أمام الجميع ومناقشتها مع المجموعة. – على المدرب/ة إدخال المستوى التحليلي للنقاش فيسأل: ماذا تعني هذه المعلومات؟ إلامَ تؤدي؟ ما هي التبعات لمشاركتنا مثل هذه التفاصيل؟ (التطرق للجانب الإيجابي والسلبي). يسأل المدرب ويسجل الإجابات مباشرة على اللّوح أمام الطلبة. من المهم مناقشة مسألة أنّه عندما يتم جمع المعلومات الخاصة بك يمكن أن يعطي ذلك الآخرين نظرة ثاقبة ومفصّلة حول حياتك، ويمكن أن تكون خاطئة للغاية أحياناً! في كلا الحالتيْن، عندما تصبح المعلومات متوفرة، فمن شبه المستحيل التحكّم بها، ويمكن أن يتم استغلالها بشكل سيء. لذا يجب التفكير جيداً قبل

	نشر أو مشاركة أي شيء على الإنترنت. أمّا الجانب الإيجابي يمكن أن يتم التطرق له للتعرّف على أشخاص مع اهتمامات مشتركة أو التمييز في مجال معين.
ملاحظات	يمكن أن يوّجّه المدرب/ المدربة سؤالاً افتتاحياً، مثل: من لديه حسابات على مواقع التواصل الاجتماعي؟ ما المواقع التي لديكم/ن حسابات عليها فيسبوك، سناب شات، تيك توك، انستغرام، إلخ...؟ ثم يطلب منهم ذكر نوعية المعلومات التي تتم مشاركتها؟ على المدرب/ة الانتباه إلى أنّ بعض الطلبة قد لا يكون لديهم/ن حسابات على مواقع التواصل الاجتماعي، والتوضيح أنّ ذلك ليس سبباً للشعور بالحرج، وعليه عندئذٍ محاولة إدماجهم/ن في النشاط من خلال إضافة أسئلة موجّهة لهم خصيصاً.

النشاط 2	**ماذا يُخبر عنك الإنترنت؟**
الفئة العمرية	11- 13 عامًا
الهدف	تعزيز توجّهات الطلاب/ات حول كميّة وطبيعة المعلومات التي يشاركونها على الإنترنت، وتأثير ذلك على الخصوصية.
الطريقة	لعبة ورق الكربون
الأدوات اللازمة	أوراق كربون، أقلام
التفاصيل	- يُقسم المدرب الطلاب/الطالبات لمجموعات صغيرة، ثم يطلب المدرب منهم كتابة نوعية المعلومات التي يشاركونها على موقع فيسبوك أو انستغرام أو غيرها على ورقة الكربون (صور شخصية، آراءهم/ن، أماكن تواجدهم، بياناتهم/ن، الاسم، تاريخ الميلاد، البريد الإلكتروني، رقم الهاتف، المدرسة، إلخ...) - يأخذ الطالب نسخته من ورق الكربون، ويأخذ الأستاذ النسخة الثانية.

	يعرض المدرب/ة المعلومات الموجودة على ورق الكربون، ويوضح أنّ الإنترنت ينسخ ويحفظ معلوماتك كورق الكربون تماماً، ثم يتم مناقشة هذه المعلومات. –على المدرب إدخال المستوى التحليلي للنقاش، فيسأل: ماذا تعني هذه المعلومات؟ إلامَ تؤدي؟ ما هي التّبعات أو العواقب لمشاركتنا مثل هذه التفاصيل (التطرق للجانب الإيجابي والسلبي معاً)، ويسأل المدرب ويسجل الإجابات مباشرة على اللوح. من المهم إجراء المناقشة إنّه عندما يتم جمع المعلومات الخاصة بك فإنّ ذلك يمكن أن يعطي الآخرين نظرة ثاقبة ومفصّلة حول حياتك، وبأنّ المعلومات التي تعطيها على الإنترنت تصبح ملك غيرك.
ملاحظات	يمكن أن يوّجّه المدرب/ المدربة سؤالًا افتتاحيًا، مثل: من لديه حسابات على مواقع التواصل الاجتماعي؟ ما المواقع التي لديكم/ن حسابات عليها فيسبوك، سناب شات، تيك توك، انستغرام، إلخ...؟ ثم يطلب منهم ذكر نوعية المعلومات التي تتم مشاركتها؟ على المدرب/ة الانتباه إلى أنّ بعض الطلبة قد لا يكون لديهم/ن حسابات على مواقع التواصل الاجتماعي، والتوضيح أنّ ذلك ليس سبباً للشعور بالحرج، وعليه عندئذٍ محاولة إدماجهم/ن في النشاط من خلال إضافة أسئلة موجّهة لهم خصيصاً.

غالبًا ما يمكن مشاركة الكثير مما نراه ونفعله في حياتنا اليومية عبر الإنترنت، بما في ذلك المعلومات والصور ومقاطع الفيديو والقصص. ويمكن أن تكون المشاركة عبر الإنترنت طريقة رائعة للبقاء على اتصال مع الأصدقاء والتعلم من الآخرين ومشاركة تجارب الحياة ببساطة. ومع ذلك، نحتاج دائمًا إلى التفكير مع من نشارك هذه المعلومات. يمكن أن تتم مشاركة المعلومات عبر الإنترنت عن قصد من خلال مشاركة منشور أو كتابة تعليق، أو عن غير قصد بواسطة أشخاص آخرين يعيدون مشاركة منشوراتك أو تعليقاتك إلى جمهور أوسع أو مختلف. وتتضمن المشاركة أيضًا المعلومات والصور ومقاطع الفيديو المتعلقة بالآخرين التي نشاركها عبر الإنترنت بالإضافة إلى أشياء تتعلق بأنفسنا.

ما الذي يشاركه الطلاب والطالبات عبر الإنترنت والذي قد يكون له عواقب غير مقصودة عليهم وعلى الآخرين؟

- معلومات شخصية

المعلومات الشخصية هي ما يحدد هويتنا، يتضمن ذلك الأسماء والمواقع وكلمات المرور وتفاصيل الاتصال، وما إلى ذلك. ويمكن مشاركة هذه المعلومات عن قصد أو عن غير قصد عبر الإنترنت من خلال الحسابات على مواقع التواصل الاجتماعي والصور ومقاطع الفيديو أو في الرسائل والمحادثات.

- الصور ومقاطع الفيديو الخاصة بهم أو بالأخرين، أو تلك التي يجدونها على الإنترنت

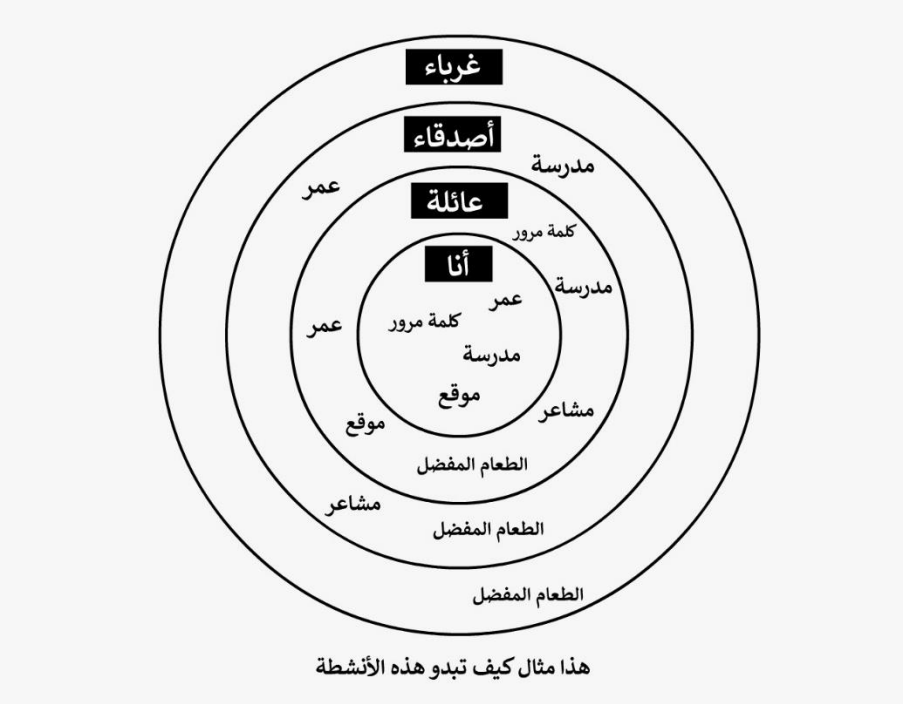
يمكن أن تشكل الصور ومقاطع الفيديو التي يلتقطها الشباب لأنفسهم خطرًا إذا كانت تحتوي على معلومات شخصية وتمت مشاركتها مع أشخاص يعرفونهم عبر الإنترنت فقط.

- كيف تقرر ما إذا كنت تريد مشاركة شيء عبر الإنترنت أم لا؟

فكّر فيما تشاركه، وما هو المحتوى، وما سبب مشاركتك لشيء ما، هل هي مفيدة، أو ضرورية، أو ممتعة للجميع ولطيفة؟

النشاط 3	**ماذا أشارك ومع من؟**
الفئة العمرية	11- 13 عامًا
الهدف	تعزيز معارف وتوجهات الطلاب والطالبات من خلال التفكير في المشاركة وإتاحة الوقت لهم للتفكير في الأشياء التي سيشاركونها مع مجموعات معينة من الناس.
الطريقة	الرسم
الأدوات اللازمة	أوراق بلون ابيض، أقلام، لوح

التفاصيل	1. اطلب/ي من الطلبة أن يرسموا 3–6 دوائر داخل بعضهم البعض (دائرة صغيرة حولها دائرة أكبر وأكبر) ارسم دائرة تمثل كلًا من الأقسام التالية: **أنا**– في هذه الدائرة اكتب/ي الأشياء التي لن تشاركها مع أي شخص، لأنه في بعض الأحيان قد تتسبب مشاركة الأشياء مع الآخرين في حدوث أذىً وانزعاج غير ضروريين. ومن المهم مراعاة الأسباب الكامنة وراء مشاركتنا لشيء ما، وتأثير ذلك على الأشخاص من حولنا. • **الأصدقاء**– في هذا القسم اكتب/ي الأشياء التي تود مشاركتها مع صديق/ة، وليكون معلومًا أن الصديق/ة هو شخص تعرفه جيدًا، وتستمتع بقضاء الوقت معه، وهو شخص يمكنك الوثوق به، ويجعلك تشعر بالأمان، ويمكنك أن تكون معه. • **العائلة**– في هذا القسم اكتب/ي الأشياء التي قد تشاركها مع عائلتك. •**الأشخاص الذين أعرفهم**– اكتب/ي في هذا القسم الأشياء التي قد نشاركها مع شخص نعرفه، وهؤلاء هم الأشخاص الذين لديك ارتباط بهم... رأيتهم من قبل وتحدثت إليهم، مثل مدرس في المدرسة، أو صديق صديقك، أو والد صديقك، إلخ... • **الأشخاص الذين لا أعرفهم**– اكتب/ي في هذا القسم الأشياء التي قد تشاركها مع شخص لا تعرفه. وهذا يشمل أصدقاء صديقك... ربما على وسائل التواصل الاجتماعي أو في مجموعة WhatsApp أو مثل لاعب آخر في لعبة عبر الإنترنت، أو حتى شخص آخر يعلّق على منشور. وتذكّر! إذا لم تقابل هؤلاء الأشخاص من قبل، فهم غرباء. 4. امنح/ي الطلبة مجموعة من الخيارات للأشياء التي قد يشاركونها. بعض الاقتراحات أدناه: الاسم، والعمر، والعنوان، والمدرسة، والموقع، وكلمات المرور، ووسائل التواصل الاجتماعي، ومشاعرك، وصور طعامك المفضّل.

	5. اطلب/ي من الطلبة أن يضعوا في الدوائر الأشياء التي سيشاركونها مع تلك المجموعة من الأشخاص.
ملاحظات	رسم توضيحي 

النشاط 4	**المعلومات الشخصية**
الفئة العمرية	11- 13 عامًا
الهدف	تعزيز معارف الطلاب والطالبات حول المعلومات الشخصية
الطريقة	نقاشٌ فعّال، وعصفٌ ذهني

الأدوات اللازمة	
التفاصيل	يقوم المدرب/ة بإدارة نقاش فعّال وعصفٍ ذهني حول المعلومات الشخصية بالاسترشاد بالأسئلة والأمثلة التالية: هل سمعت عن المعلومات الشخصية من قبل؟ ما هي المعلومات الشخصية؟ وكيف تصفها لشخص لم يسمع بها من قبل؟ المعلومات الشخصية هي أي جزء من المعلومات يكون خاصًّا أو فريدًا بالنسبة لنا. إنها معلومات تكشف شيئًا عنّا، ويمكن أن تساعد شخصًا ما على معرفة المزيد عنا... غالبًا ما يتم وصفها بأنها "معلومات يمكن تحديدها" مما يعني أنّه يمكن لأيّ شخص معرفة الفرق بيننا وبين شخص آخ. ما الذي يعتبر معلوماتك الشخصية؟ اسمك، وعمرك، وعنوانك، ومدرستك، وموقعك، وكلمات المرور، وأسماء المستخدمين، وعلامات اللاعب، والحسابات على مواقع التواصل الاجتماعي، وعناوين البريد الإلكتروني، وما إلى ذلك. إذا كان بإمكانك تحديد شخص من المعلومات التي يتم مشاركتها، فقد تكون هذه هي بيانات شخصية. لذلك، من المهم تضمين الصور ومقاطع الفيديو ولقطات الشاشة في المناقشات حول المعلومات الشخصية. كيف وأين تتم مشاركة المعلومات الشخصية عبر الإنترنت؟ يمكن مشاركة المعلومات الشخصية على الملفات الشخصية، وفي الصور ومقاطع الفيديو، أو من خلال الرسائل والتحديثات والحالات، أو حتى من خلال الدردشة الصوتية (في الألعاب على سبيل المثال)، وعلامات الموقع. هل يمكنك التفكير في مثال بحيث يمكننا مشاركة المعلومات الشخصية عبر الإنترنت عن قصد؟ مثال على ذلك هو عندما نقوم بالتسجيل في حساب جديد حيث يتعين علينا إكمال نموذج نشارك فيه المعلومات الشخصية، مثل: الاسم وعنوان البريد الإلكتروني، وما إلى ذلك.

	5. هل يمكنك التفكير في مثال بحيث يمكننا مشاركة المعلومات الشخصية عبر الإنترنت عن طريق الخطأ أو دون إدراك؟ مثال على ذلك هو عند مشاركة صورة أو مقطع فيديو يحتوي على معلومات شخصية في الخلفية، ويمكن أن تكون كشهادة على الحائط، أو زيٍّ مدرسي معلّق، أو لافتة تدل على مبنى أو شارع، بحيث يمكن التعرف عليها. وفي بعض الأحيان نقوم بمشاركة الصور ومقاطع الفيديو دون النظر عن كثب إلى ما قد يكون في الخلفية. 6. بمن يمكننا الوثوق بمعلوماتنا الشخصية؟ الأشخاص الذين نعرفهم بالفعل في العالم الحقيقي، على سبيل المثال: أصدقاء المدرسة والعائلة والمعلمين/ات وموظفو الدّعم، إلخ... 7. من هم الأشخاص الذين لا يمكننا الوثوق بمشاركة معلوماتنا الشخصية معهم؟ أي شخص لم نلتقِ به بالفعل من قبل؛ لأنّه من الصعب أن نعرف على وجه اليقين شخصيتهم الحقيقية، وغالبًا ما نسمي هؤلاء الناس "غرباء". 8. هل من المقبول مشاركة المعلومات الشخصية عن أشخاص آخرين؟ يجب أن نسأل دائمًا شخصًا ما إذا كان الأمر مقبولًا لديه قبل أن نشارك أي شيء عنه عبر الإنترنت. سيكون هذا هو نفسه بالنسبة للمعلومات التي نشاركها بشكل عام على وسائل التواصل الاجتماعي أو الألعاب، أو بشكل خاص على تطبيقات المراسلة.
ملاحظات	

عند رؤيتنا لمشاركات وتعليقات وصور شخصٍ معيّن، نحن نبني افتراضاتٍ عنه/ها، وقد لا تكون صحيحة دائمًا، خاصّة إذا كنا لا نعرف هذا الشخص، وذلك لأنّ ما نراه على الإنترنت ليس سوى جزءٍ يسير من شخصيته/ها و اهتماماته/ها. وقد لا يُظهر

هذا الشخص يظهر شخصيته/ها الحقيقية، أو أنّه/ها شارك/ت مشاعر مؤقتة راودته/ها فقط في لحظة نشره للمشاركة، بحيث لا يمكننا أن نعرف حقًا من هو، أو كيف يشعر حتى نتعرف عليه شخصيًا، وحتى في تلك الحالة تتطلب معرفته/ها فعليًا بعض الوقت.

هناك الكثير من المعلومات الشخصية التي يمكن العثور عليها على الإنترنت، وقد يدفعنا بعضها لتكوين نكون آراء وافتراضات معيّنة حول أشخاص قد يتضح فيما بعد أنها خاطئة. ويمكن للأشخاص المختلفين رؤية نفس المعلومات واستخلاص استنتاجات مختلفة تمامًا، ولذا لا تفترض بأن الأشخاص على الانترنت سيرونك بالطريقة التي تعتقد أنك تقدم نفسك بها.

يمكن أن يكون العالم الافتراضي مختلفًا تمامًا عن العالم الحقيقي. هل صديقك عبر الإنترنت هو الشخص الذي تعتقد!؟

لا تقابل أبدًا صديقا "افتراضيًا" في الحياة الواقعية دون مناقشة الأمر أولًا مع شخص بالغ. وإذا كنت توافق على مقابلة صديق "من الإنترنت" خارج الإنترنت، خذ احتياطات السلامة، بصرف النظر عن عمرك، وأخبر مَن حولك عن مكان اللقاء أو خذ شخصا آخر معك.

النشاط 5	**من هو/ هي؟؟**
الفئة العمرية	14–16 عامًا
الهدف	تعزيز توجّهات الطلاب/ات حول "ليس كل ما هو موجود على الانترنت حقيقي بالضرورة" وإن أحكامنا واستنتاجاتنا عن الأشخاص على الإنترنت قد تكون خاطئة.
الطريقة	عمل مجموعات، دراسة شخصيات
الأدوات اللازمة	ورقة الشخصيات الوهمية لتوزيعها على الطلاب، ورقة حقيقة الشخصيات للمدرب/ة
التفاصيل	يتم تنفيذ النشاط على قسميْن، كالتالي: **القسم الأول:** يتوزّع الطلاب/ات إلى مجموعات، وتحصل كل مجموعة على إحدى الشخصيات وتكتب وصفًا سريعًا يجيب عن السؤال: "من هو/هي هذا الشخص برأيك؟"

	يدرس الطلاب مجموعة من المعلومات الشخصية على الإنترنت حول شخصية وهميّة من أجل محاولة استنتاج أمور عنها. في ما يلي الأسئلة التي سنقوم بمناقشتها: ما الذي يمكننا معرفته عن شخص ما من معلوماته/ها الشخصية؟ ما هي الافتراضات التي يمكننا أن نكوّنها من المعلومات الشخصية، حتى لو لم نكن متأكدين؟ هل نعرف كيف تم جمع هذه المعلومات؟ كيف يمكننا تحديد المصدر؟ بعد ذلك، يقوم المدرب بكشف حقيقة هذه الشخصيات ثم نقاش: أيّ من الافتراضات كانت صحيحة، وأيّها لم تكن كذلك؟ لماذا ولم لا؟ **القسم الثاني:** دعونا نلقي نظرة أخرى على الملف الشخصي من وجهة نظر شخصيات النشاط السابق، هل تعتقد أنهم يريدون كشف كل هذه المعلومات الشخصية؟ لماذا ولم لا؟ كيف يمكن للآخرين رؤية هذه المعلومات؟ كيف يمكن استخدام هذه المعلومات من قبل الآخرين؟ ما هي أهم استنتاجاتك من النشاط؟ لماذا قد ترسم المعلومات التي رأيناها صورة غير مكتملة؟ ما هي برأيك عواقب تكوين شخص ما لرأي سلبي عنك بناءً على المعلومات الموجودة على الإنترنت؟ **الشخصيات الوهمية**


لينا
الحفلة تبدو جميلة وانتم جميعا رائعون
افضل الطرق لتخلص من حبوب الوجه
اخي الصغير فادي مزعج جدا
ما اجمل الطبيعة هنا
مؤتمر المصممين الشباب في الجامعة
لقد شاهدت واخيراالفيلم الجديدروووعة
عبير
فزنا في اللعبة، بقي لعبة واحدة للوصول للبطولة ، علي التمرن اكثر
انا اكره الحفلات الموسيقية المدرسية #لن_اذهب
: كلية العلوم ، نابلس
10 علامات تدل على ان اهلك لا يحبونك
سأذهب الى البحر الميت مع عائلتي يوم السبت ، سأقضي وقتا ممتعا
معجبة بهذه الفرقة الكورية اللطيفة

حقيقة الشخصيات:

تذكر عدم البدء بالقراءة حتى تنتهي كل المجموعات من كتابة الوصف.

لينا: هي طالبة في المدرسة الثانوية، وتخطط للالتحاق بالكليّة العام المقبل، حيث ترغب في دراسة الهندسة، مجال اهتماماتها: العائلة والعمل التطوعي والثقافة الشعبية والموضة.

عبير: هي لاعبة كرة سلة محترفة في فريق المدرسة الثانوية، تبلغ من العمر 15 عامًا وتسكن في نابلس، لديها أخت عمرها 8 أعوام، مجال اهتماماتها: كرة السلة ودراسة الفن وعزف الجيتار وقضاء الوقت مع الأصدقاء.

احمد: عمره 14 عامًا، انضم مؤخرًا لفريق كرة القدم ولديه قطّة، وهو ماهر جدًا في الرسم، يحب قضاء عطلة الأسبوع في البرمجة، مجال اهتماماته: التكنولوجيا، ومتابعة فريقه في كرة القدم والحيوانات.

ملاحظات

النشاط 6	**من هو/ هي؟ (صندوق الحقيقة)**
الفئة العمرية	**11-13 عامًا**
الهدف	يجب أن ندرك أن الأحكام والاستنتاجات عما ينشره الآخرون قد تكون خاطئة تمامًا. تعزيز توجهات الطلبة بأنّ الشخصيات في العالم الافتراضي قد لا تكون حقيقية.
الطريقة	لعبة صندوق الحقيقة
الأدوات اللازمة	صندوقان: الصندوق الأول: موجود فيه معلومات عن حسابات شخصية وهمية. الصندوق الثاني: صندوق الحقيقة يوجد فيه المعلومات الحقيقية عن نفس الشخصيات.
التفاصيل	**القسم الأول:** يتم وضع صندوقين أمام الطلاب/ الطالبات الصندوق الأول هو صندوق معلومات الملف الشخصي لشخصيات وهمية، والصندوق الثاني هو صندوق الحقيقة (يتم استخدام نماذج الشخصيات من النشاط السابق) يختار الطلاب مجموعة من الأوراق من داخل الصندوق الأول حول شخصية على مواقع التواصل ويقرؤونها أمام زملائهم الطلاب. فيما بعد، يقوم مجموعة أخرى من الطلاب بأخذ المعلومات الحقيقية من صندوق الحقيقة عن الشخصية. **في ما يلي الأسئلة التي سنقوم بمناقشتها:** ما الذي يمكننا معرفته عن شخص ما من معلوماته الشخصية؟ ما هي الافتراضات التي يمكن أن نكوّنها من المعلومات الشخصية، حتى لو لم نكن متأكّدين؟ هل الحسابات للأشخاص على الإنترنت سليمة دومًا؟ بعد ذلك يقوم المدرب بكشف حقيقة هذه الشخصيات. ثم نقاش: هل الشخصيات الموجودة في عالم الإنترنت حقيقية؟ ماذا يؤثر علينا ذلك؟ وماذا يعني؟
ملاحظات	

النشاط 7	**كم نحن مكشوفين/ ات!**
الفئة العمرية	11–16 عامًا
الهدف	إدراك أثر كشف ومشاركة المعلومات على الإنترنت بالنسبة للطلبة.
الطريقة	اختبار ورقي
الأدوات اللازمة	أوراق اختبار (كم نحن مكشوفين!) لجميع الطلبة
التفاصيل	يقوم المدرب بتوزيع الاختبار على الطلاب والطالبات لإدراك وفحص كم هم مكشوفين على فيسبوك، ويطلب منهم تعبئته مع إعطائهم وقتًا محدّدًا للإنهاء، وتوضيح أنه في حال كان هنالك أكثر من خيار، فيتم اختيار الخيار ذي العدد الأكبر. استخدام نتائج الاختبار كقاعدة لفتح نقاش حول عواقب كشف المعلومات الشخصية. يفسر المدرّب/ المدربة للطلاب كيف يمكن أن تكون صورهم ومعلوماتهم الشخصية وسيلة لاستغلالهم عبر الإنترنت، ونعلّمهم ألّا يقوموا بنشر صورهم فورًا، أو على الأقل عندما يعتقدون أنّ الصور قد لا تكون مناسبة.
	تابع نشاط رقم 7 (الاختبار) ***كم مرة تنشر على فيسبوك؟** 1. ليس لدي حساب فيسبوك. 2. مرّة كل شهر. 3. مرّة في الأسبوع، أو مرّة كلّ يوم. 4. عدّة مرات في اليوم. ***أي من معلوماتك التالية عامة على فيسبوك؟**

1. اسم مستعار (ليس اسمي الحقيقي).

2. اسمي الحقيقي/ تاريخ الميلاد/ المدينة الأصلية/ نبذة عنّي/ الجنس/ العنوان.

3. المدينة الحالية/ الأسرة/ التعليم/ العمل/ الصفحات التي تعجبك/ الأسعار المفضلة/ البريد الإلكتروني/ الأحداث/ وجهات النظر السياسية/ وجهات النظر الدينية/ رقم الهاتف/ المعلومات الموجودة في الصور.

*** مع من تشارك المحتوى على Facebook ؟**

مجموعات محدّدة من الأصدقاء.

1. الأصدقاء.

2. أصدقاء الأصدقاء.

3. عالم الإنترنت الواسع (أي العام كلّه).

- **ما نوع المحتوى الذي تشاركه/ تنشره على Facebook ؟**

1. منشورات

2. وضع إشارة (Taq) للأصدقاء في المنشورات، ومشاركة الصفحات التي تريدها.

3. الصور ومقاطع الفيديو/ الموقع الحالي.

4. الأماكن التي تزورها (CHECK-IN)/ منشور عن آرائي السياسية/ الدينية.

***لماذا تستخدم فيسبوك؟**

1. مشاركة صور القطط.

2. تحديث/ التواصل مع الأصدقاء المقرّبين.

3. التعرّف على أشخاص جدد وتسويق.

4. إيجاد أشخاص وصفحات تشاركك نفس اهتماماتك.

*** النتيجة**

06-09 مكشوف بشكل منخفض.

	13–09 مكشوف بشكل متوسط، هل هناك مناطق يمكنك تقليلها؟ 20–14 مكشوف بشكل مرتفع جدًا ويمكن بالتأكيد تقليل ذلك.
ملاحظة	تم وضع اختبار على فيسبوك، لكن من الممكن تعديله ليتناسب مع أي موقع أو تطبيق آخر.

يختلف السلوك وتختلف التصرفات المطلوبة باختلاف المواقف، وذلك في عالم الانترنت وخارجه، ومن المهم دائمًا احترام خيارات الآخرين المتعلّقة في الخصوصية، حتى لو كانت مختلفة عن خياراتنا.

النشاط 8	**ما الذي يجدر فعله؟**
الفئة العمرية	11 –16 عامًا
الهدف	توجيه الطلبة حول أهمية احترام خصوصية الآخرين.
الطريقة	مناقشة سيناريوهات.
الأدوات اللازمة	سيناريوهات الخصوصية "ما الذي يجدر فعله؟"
التفاصيل	سنستعرض أربعة سيناريوهات ونتحدث عن احترام الخصوصية الخاص بكلّ منها. توزيع الطلاب لأربع مجموعات، بحيث تقوم كلّ مجموعة بمناقشة وإيجاد الحلّ لسيناريو واحد، ثم يتم مناقشة السناريوهات بشكل جماعي، وذكر أمثلة أخرى من قبل الطلاب والطالبات يعتبرونها انتهاكًا لخصوصية الآخرين. **أمثلة على سيناريوهات لاحترام خصوصية الآخرين:** 1. "هيا ودُنيا" صديقتان مذ كانتا في السابعة من العمر، تتشارك هيا ودنيا كلّ أسرارهما معًا، "هيا ودُنيا" في المرحلة الثانوية الآن، وقد نشب بينهما خلاف، فقامت دُنيا بكتابة منشور يكشف أسرار هيا على مواقع التواصل الاجتماعي. كيف شعرت هيا بعد ذلك؟ ما رأيك بتصرف دُنيا؟

	ماذا يتوجب على هيا فعله بعد ذلك؟ 2. "تمارا ولُجيْن" صديقتان حميمتان، وتقضيان الكثير من الوقت معًا، يومًا ما كانتا في الرحلة المدرسية، التقطتا صورًا ومقاطع فيديو لهما في الرحلة، في وقت لاحق من ذلك المساء قامت تمارا بمشاركة صور من الرحلة المدرسية برفقة صديقتها لُجيْن على مواقع التواصل الاجتماعي، علمًا أن لُجيْن طلبت من تمارا ألّا تنشر أيًّا من هذه الصور. كيف شعرت لُجيْن بعد هذا؟ ما الذي كان بإمكان تمارا فعله بشكل مختلف؟ الآن وقد حدث هذا بالفعل، ما الذي يمكن أن تفعله تمارا لتحسين الوضع؟ كيف يمكن أن تتحقّق تمارا إذا كان من المقبول مشاركة صورة لغيرها قبل أن تفعل ذلك؟ 3. إذا علمتَ بأن أحد الطلاب أنشأ حسابًا مزيّفًا على أحد مواقع التواصل الاجتماعي منتحلًا شخصية طالب آخر بطريقة سلبية. ما الذي عليك فعله؟ 4. على مجموعة الواتساب للصف طلبت ميساء رقم الهاتف وعنوان المنزل لزميلتها سمر، وعلى الفور قامت ميساء بأرسالها على المجموعة علمًا أنه يوجد 20 شخصًا على هذه المجموعة. هل تصرف ميساء صحيح؟ ما الذي كان بإمكان ميساء أن تفعله؟
ملاحظات	

يمكنك حماية خصوصيتك من خلال عدم مشاركة إلّا ما ترغب/ين فعلًا بمشاركته، واختيار ما تريد/ين نشره أو مشاركته على الإنترنت بحذر، كما يمكننا عمل بعض الإجراءات البسيطة في حساباتنا على الإنترنت لتوفير خصوصية أكبر لنا من خلال تحديد من يمكنه رؤية ما ننشره ومع من نتواصل، وغيرها.

عندما تستخدم تطبيقا او موقعا على الويب ابحث عن خيارات مثل "حسابي" و" الإعدادات"، ستجد أن هنالك إعدادات الخصوصية والأمان التي تتيح لك اختيار المعلومات التي تظهر في ملفّك الشخصي، مثل: الأشخاص الذين يستطيعون رؤية مشاركاتك، أو صورك أو فيديوهاتك، أو أي محتوى آخر تشاركه.

بعد تعلّم استخدام إعدادات الخصوصية هذه والحرص على تحديثها بشكل مستمر، ستتمكن/ين من إدارة خصوصيتك وأمانك على الإنترنت، ومن الممكن مشاركة الأهل في اتخاذ هذه الخيارات ومناقشة إعدادات الخصوصية والأمان المناسبة لك معهم. ولكن، تذكّر/ي بأنّ أهم إعدادات الأمان موجودة في ذهنك، حيث أنتَ/أنتِ من تقرر/ين حجم المعلومات الشخصية التي تريد/ين مشاركتها، وكذلك التوقيت المناسب والأشخاص المناسبين.

(ممكن نقل هذا النشاط في جزء الأمان الرقمي)

النشاط 9	**إعدادات الخصوصية والأمان**
الفئة العمرية	11-16 عامًا
الهدف	معرفة الطلاب كيفية ضبط إعدادات الخصوصية لزيادة الحماية والخصوصية على الإنترنت
الطريقة	عرض على الشاشة
الأدوات اللازمة	جهاز حاسوب، بروجكتر
التفاصيل	استخدام جهاز حاسوب للمدرسة لتوضيح وسائل تخصيص إعدادات الخصوصية وكيفية الوصول إليها. بحيث يقوم المدرب بالدخول إلى أحد الحسابات على أحد مواقع التواصل الاجتماعي (يفضل أن يكون حسابًا مخصّصًا للتدريبات) يقوم بالدخول للإعدادات والشرح للطلاب- خطوة بخطوة- كيفية ضبط الإعدادات للتقليل من وصول الآخرين للمعلومات, يمكن كذلك أن يطلب المدرّب من الطلاب/ الطالبات محاولة ضبط الإعدادات بأنفسهم/ن ليكون التمرين تفاعليًا أكثر، وأن يتناوب بعض الطلاب لضبط الإعدادات على الحساب.

ملاحظات	فيما يلي أدلّة للمساعدة في كيفية ضبط إعدادات الخصوصية على بعض مواقع التواصل الاجتماعي، ويفضل أن يقوم الطلاب/ الطالبات في تطبيق ذلك عمليًا مع المدرب/ ة إن أمكن. - دليل أمان فيسبوك https://securityinabox.org/ar/guide/social-networking/web/#%D8%AF%D9%84%D9%8A%D9%84-%D8%A3%D9%85%D8%A7%D9%86-%D9%81%D9%8A%D8%B3%D8%A8%D9%88%D9%83 - دليل أمان انستغرام https://www.facebook.com/help/instagram/377830165708421/ - دليل أمان سناب شات https://www.snap.com/ar/safety/safety-center/

من المهم التوضيح للطلاب أنّ حماية الخصوصية من الأفراد مختلفة تماماً عن حماية الخصوصية من الشركات. الفرق بين الفرد والشركة هو الهدف من جمع المعلومات. حين ينتهك فردٌ خصوصيتك، فإن الهدف الرئيسي عادة هو لربحٍ مادّي مباشر منك (ابتزاز) أو إجبارك على تصرف لا تودّه أو بهدف التخريب. بينما حين تقوم شركة بجمع بيانات عنك فإن الهدف يكون أكثر بهدف ملائمة بيع منتجات معينة لك، أو الكشف عن مضامين ذات صلة باهتمامك حتى يتأكدوا أنك ستقضي وقتاً أطول على موقعهم، وربما تصرف نقودًا بشراء منتجات عن طريقهم. في الحالتين هنالك انتهاك للخصوصية، لكن الطريقة التي يتم بها

ذلك تختلف، فالفرد حين يخترق خصوصية آخر يقوم بذلك بطريقة غير قانونية، مثل: إخفاء معلومات معينة أو انتحال شخصية، أو إرسال تروجانز، إلخ... بينما الشركات تقول بصريح العبارة أنها ستستخدم معلوماتك للأهداف المذكورة أعلاه.

بعض الأشخاص قد لا يهتمّون بحماية خصوصيتهم من الشركات، وهذا حقّ فردي. لكنْ، من المهم الإشارة أنهم مستقبلاً سيكونون عرضة بشكل أكبر وبشكل أسهل لدفعهم للقيام بتصرفات معينة، أو شراء منتجات معيّنة؛ لأن الشركة تمكنت من معرفة كيف تفكر، وما هو المهم بالنسبة لك. من الممكن عرض جزء من فلم social dilemma حيث يتحدث مجموعة من المدراء والخبراء من انستغرام وفيسبوك وغيرها من المنصّات عن تحديد إتاحتهم لهذه المواقع لأطفالهم لحمايتهم من هذا النوع من انتهاك الخصوصية.

عندما تقوم باستخدام التطبيقات و مشاركة منشورات وغيرها، يتم تحليل نشاطك بواسطة شركات التكنولوجيا، أو وسطاء البيانات لمنحهم فكرة أفضل عن هويتك، حتى يتمكنوا من تقديم إعلانات ومحتوىً أكثر تخصيصًا لك.

يُعدّ الحصول على إعلان على Facebook لتلك الأحذية التي كنت تبحث عنها عبر الإنترنت أمرًا واحدًا، ولكن هناك الكثير من الطرق الأخرى التي يتم من خلالها استخدام عادات التصفّح ونشاط وسائل التواصل الاجتماعي والمعلومات الأخرى التي قد تؤثر عليك في الحياة الواقعية، وربما يعرفون أشياء عنك لن تخبرها حتى لأصدقائك المقربين أو لأفراد أسرتك، أو أنها تستخلص استنتاجات عنك لم توافق عليها أو تتماشى معك.

الأمان الرقمي للوقاية من العنف الإلكتروني

من المهم أن يفهم الطلاب أنّ المحتوى الذي يعثرون عليه على الإنترنت ليس بالضرورة صحيحًا أو موثوقًا، وقد يتضمن محاولات ضارة لسرقة معلوماتهم/ن أو هويتهم/ن، وتدفع الأساليب المتبعة في عمليات التصيّد الاحتيالي وغيرها من عمليات الاحتيال على الإنترنت مستخدمي الإنترنت من جميع الأعمار للاستجابة لأمور من أشخاص لا يعرفونهم، وأحيانًا من أشخاص ينتحلون هوية أشخاص يعرفونهم، وقد يؤدي ذلك في نهاية المطاف لإيذائهم وابتزازهم، لذا من المهم التنبّه لمحاولات التصيّد والحذر منها.

ماهو التصيّد الاحتيالي؟

التصيّد الاحتيالي هو عندما يحاول شخص ما سرقة معلومات كتسجيل الدخول، أو الحساب الخاصة بك في البريد الإلكتروني، أو رسالة نصيّة، أو أي اتصال على الإنترنت، ويتم ذلك من خلال التظاهر بأنّه شخصٌ تثق به، وكأن الرسالة مرسلة من شركات موثوقة أو وحكومية أو من أشخاص تعرفهم، لكنّها في الحقيقة مواقع وهمية وزائفة.

يمكن لرسائل التصيّد الاحتيالي المرسلة بالبريد الإلكتروني والمواقع غير الآمنة التي يحاولون توجيهك إليها، أو الملفّات المرفقة التي يحاولون إقناعك بفتحها أن تزرع الملفات الضارة "الفيروسات" في جهاز الكمبيوتر الخاص بك. وعادة ما تستخدم بعضُ الفيروسات قائمةَ جهات الاتصال لاستهداف أصدقائك وأفراد عائلتك بنفس الطريقة، أو في هجوم احتيالي أكثر تخصيصًا. كما قد تحاول أنماطٌ أخرى من عمليات الاحتيال خداعك لتحميل برامج ضارة أو برامج غير مرغوب فيها من خلال إعلامك بوجود خطأ ما في جهازك.

تذكّر! لا يمكن لأي موقع ويب أو إعلان معرفة ما إذا كان هناك أي خطأ في جهازك.

التصيّد يتم غالبًا من خلال رسائل إلكترونية تحاول خداعك لفتح رابط أو تحميل ملف أو حل مشكلة برنامج ما.

وقد تكون بعض محاولات التصيّد الاحتيالي زائفة بوضوح، وقد يكون بعضها خادعًا ومُقنعًا، مثال ذلك: عندما يرسل إليك الشخص المحتال رسالة تتضمن بعض معلوماتك الشخصية وهذا ما يسمى بالتصيد الإلكتروني الموجه، وقد يكون من الصعب رصده؛ لأنّ استخدام معلوماتك يجعل الأمر يبدو كما لو أنّ المرسل يعرفك حقًا.

وفيما يلي بعض الأمور لتجنب الوقوع في فخّ التصيّد:

- <u>كن حذرًا من مشاركة المعلومات</u>

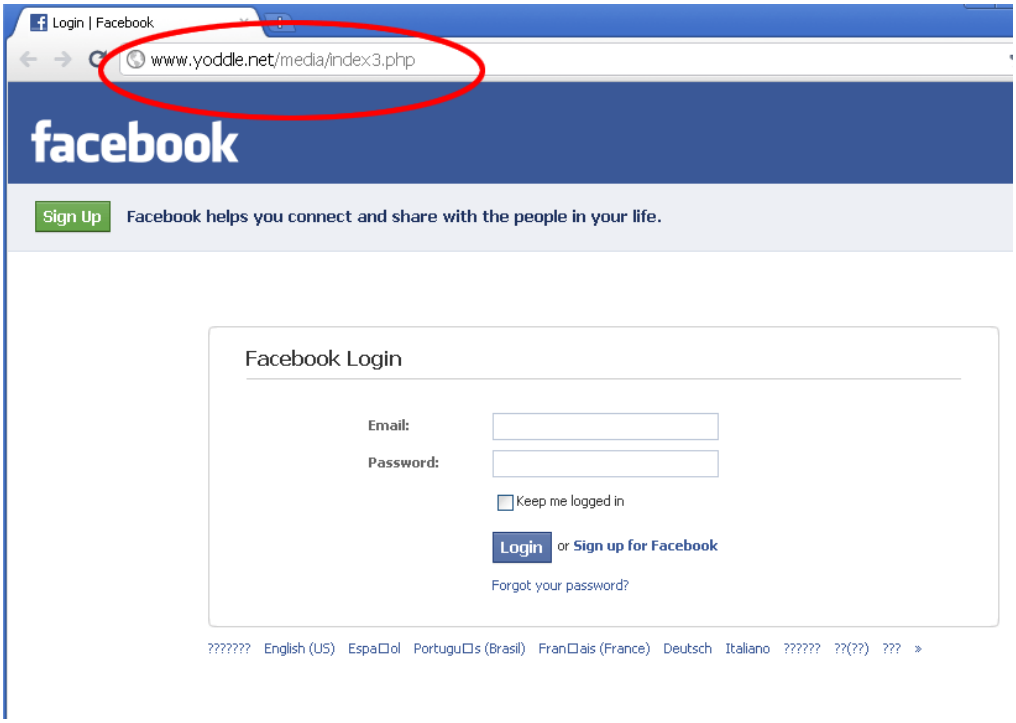
احذر/ي من أي رسالة على البريد الإلكتروني أو على وسائل التواصل الاجتماعي، أو في المحادثات الخاصة التي يُطلب منك مشاركة معلوماتك الخاصة مع أطراف حتى وإن كانوا معروفين بالنسبة لك.

- <u>لا تستجب/ي للضغوط</u>

يستغل المتطفّلون/ات والأشرار بعضَ الحيل للضغط عليك من أجل الاستجابة في مشاركة معلوماتك معهم، يستخدمون في ذلك "إستراتيجية التخويف"؛ حيث يخبرونك كذبًا بأنّ الحساب سوف يتوقف أو يتعطل، وأنّه لن يتم تفعيل الخدمة حتى تقوم بتحديث معلوماتك الشخصية والحسّاسة، وليكن معلومًا أن الغرض من هذه الإستراتيجية استغلال خوفك من توقف حسابك أو الخدمة. لذلك، لا تُشارك معلوماتك معهم، وقم بالاتصال بالقائمين على الموقع الإلكتروني أو الخدمة مباشرة للتأكد من صحّة هذه الرسالة

- <u>لا تثق/ي بالروابط</u>

بعض الأحيان تصلك روابط يتم خلالها الطلب منك الدخول إليها من أجل تسجيل الدخول على الموقع.



الملاحظات:

١– شكل الموقع: هذا هو الشكل الخاص لموقع Facebook ولم يتغير شيء.

٢– الرابط: هذا الرابط– في الدائرة الحمراء– ليس تابعًا لموقع Facebook.

الوصلة الحقيقة هي: https://www.facebook.com

تذكّر! يُفضّل دائمًا كتابة اسم الموقع بنفسك بدل النقر على أي رابط أو وصلة.

- شهادة الأمان Security certificate

تأكد/ي دائمًا بأنّ الموقع الإلكتروني الذي قمت بالدخول إليه يحتوي على SSL/TLS وهي شهادات الأمان، والتي تقوم بتعمية أو ما تُعرف باسم "تشفير" الاتصال بينك وبين الموقع الإلكتروني الذي تستخدمه.

مثال: عندما تدخل على موقع https://twitter.com

سوف يحتوي الموقع على شهادة الأمان وهي حرف (S) بعد البروتوكول http

- مصدر الرسالة البريدية:

تأكد/ي دائمًا من مصدر الرسالة، حيث إن شركة فيسبوك وغيرها من الشركات لديها عنوانين محددة يتم استخدامها في إرسال الرسائل.

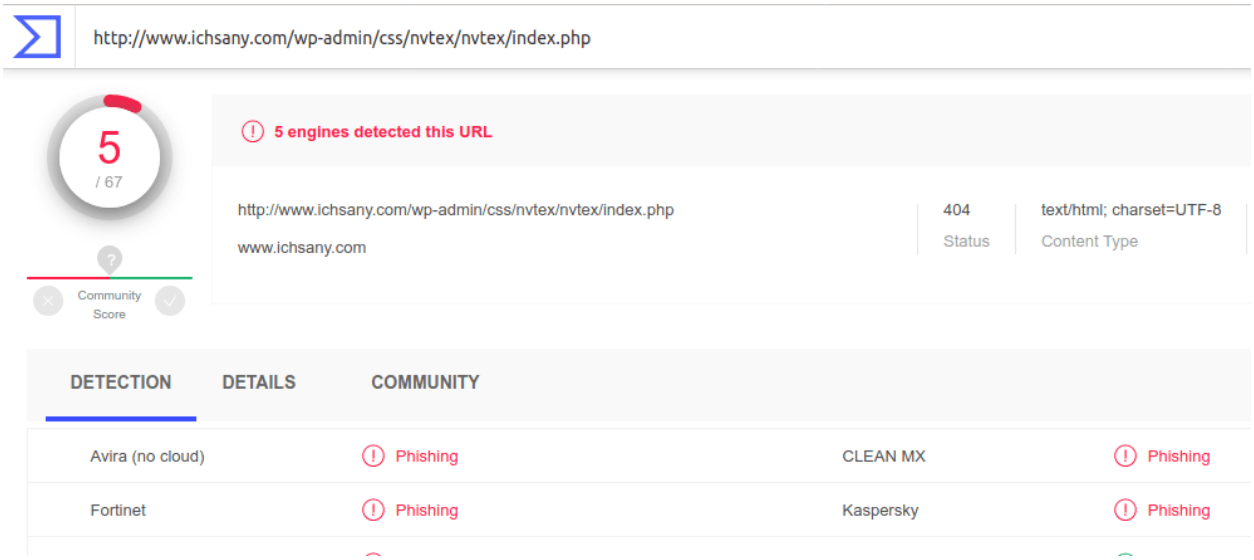
مثال : Info@twitter.com أو security@facebookmail.com

حيث إنّ الرسائل الوهمية تحاول أن تستخدم عنوانين وهمية وقد تكون مشابهة للحقيقيّة.

- فحص الروابط:

- إذا كنت تشك/ين في ملف أو رابط، قم/قومي بفحصه هنا: https://www.virustotal.com مع العلم أن هذا الموقع لا يستطيع كشف جميع الفيروسات.

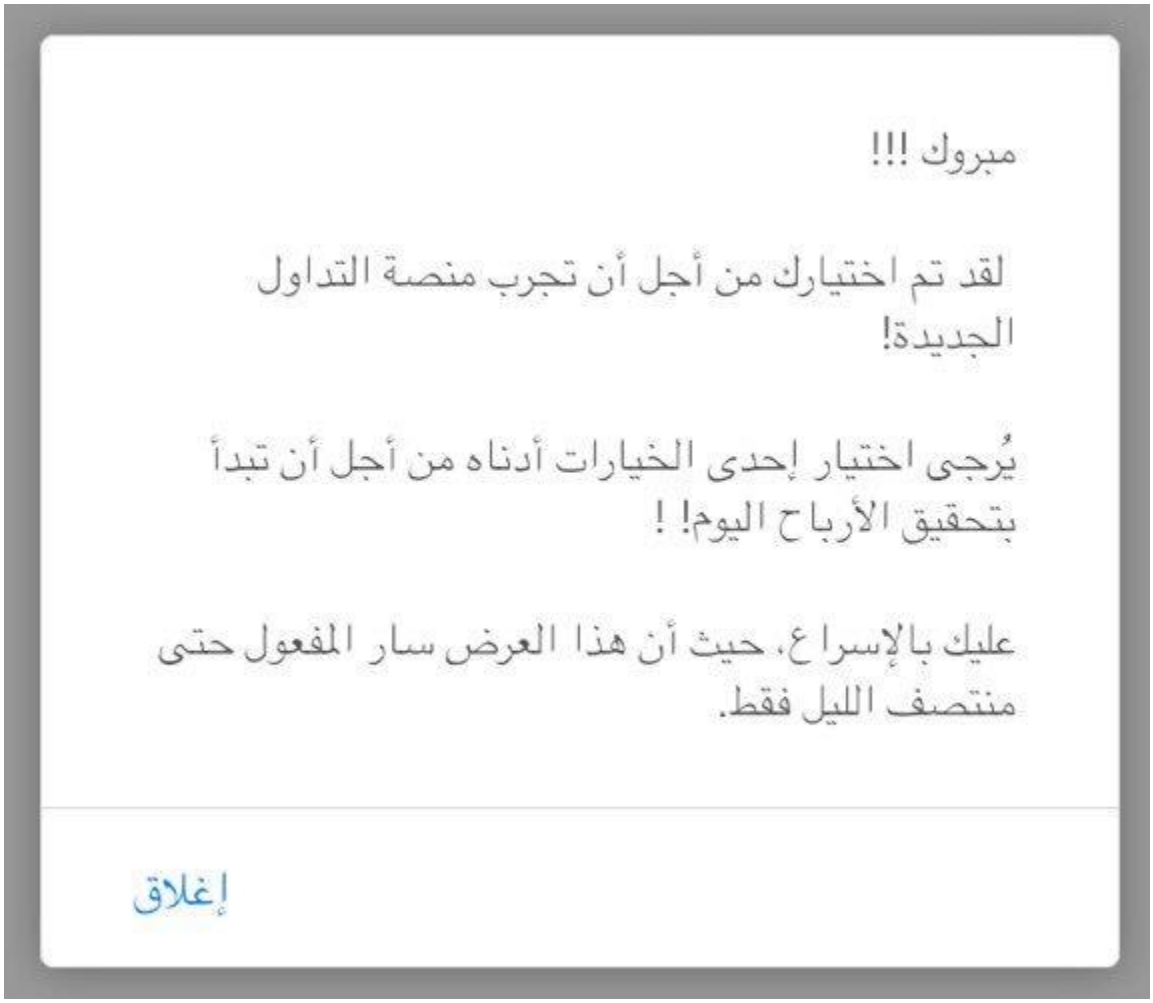
مثال : http://www.ichsany.com/wp-admin/css/nvtex/nvtex/index.php



كيف يتم الاستخدام: إذا كنت ترغب باستخدام الموقع، انقر في الصفحة الأولى على URL ومن ثم قم بوضع اسم الرابط/ الوصلة التي ترغب في فحصها.

- الجوائز الوهمية:

يستخدم المهاجمون طرق احتيال مختلفة من أجل استهداف الأشخاص، وتكون هذه الطرق في بعض الأحيان مرتبطة بالأوضاع الحالية في البلد أو في العالم. سوف يطلب منك النقر على روابط/ وصلات للحصول على جوائز وهمية (أموال، حزم إنترنت مجانية، حواسيب وهواتف، وغيرها)



- انتحال الشخصية:

قد يتمّ إرسال هذه الرسائل عن طريق بريد إلكتروني معروف لديك (صديقك أو أحد أقاربك)، ولكنْ، في بعض الأحيان يتم استخدام طريقة "انتحال الشخصية" وهي طريقة يتم فيها استغلال بريد إلكتروني لأشخاص أنت تعرفهم من أجل التواصل معك.

إذا تم طلب معلومات حساسة أو شخصية أو غيرها فعليك أن تتأكّد قبل التجاوب مع هذا الطلب بأنّ الشخص الذي اتصل بك لم يتمّ اختراق بريده الإلكتروني، أو لم يتم انتحال شخصيته.

ماذا تفعل إذا كنت ضحيّة "التصيد" Phishing؟

- قم/ي بتغيير كلمة السر حالًا.
- أبلغ/ي جميع الأصدقاء على وسائل التواصل الاجتماعي بهذه الحادثة، واطلب/ي منهم التوقف عن التواصل مع حسابك حتى يتم حمايته.
- اطلب/ي المساعدة من إدارة المواقع أو اتصل/ي بالبنك لوقف الخدمة أو لإبلاغهم بالحادثة.
- حاول/ي تحذير الآخرين حول الموقع أو الخدمة أو البريد الإلكتروني الوهمي/ الزائف الذي وصلك، أو الذي قمت بالدخول إليه.

النشاط 1	**مفهوم التصيّد الاحتيالي الإلكتروني**
الفئة العمرية	11- 16 عامًا
الهدف	تعزيز مهارات ومعارف الطلاب في التعرّف على مفهوم التصيد الاحتيالي.
الطريقة	عرض فيلم التصيد
الأدوات اللازمة	جهاز حاسوب، بروجكتر
التفاصيل	عرض فيلم يوضح مفهوم التصيّد الاحتيالي، ونناقش بعد ذلك المفهوم مع جميع طلاب الصف. بالإضافة للنقاط المذكورة في الأعلى.
ملاحظات	

قبل النقر على الرابط أو إدخال كلمة المرور الخاصة بك في موقع لم تزره من قبل، من المستحسن التفكير في بعض الأسئلة حول تلك الرسالة الإلكترونية أو صفحة الويب، وفي ما يلي بعض الأسئلة الممكنة:

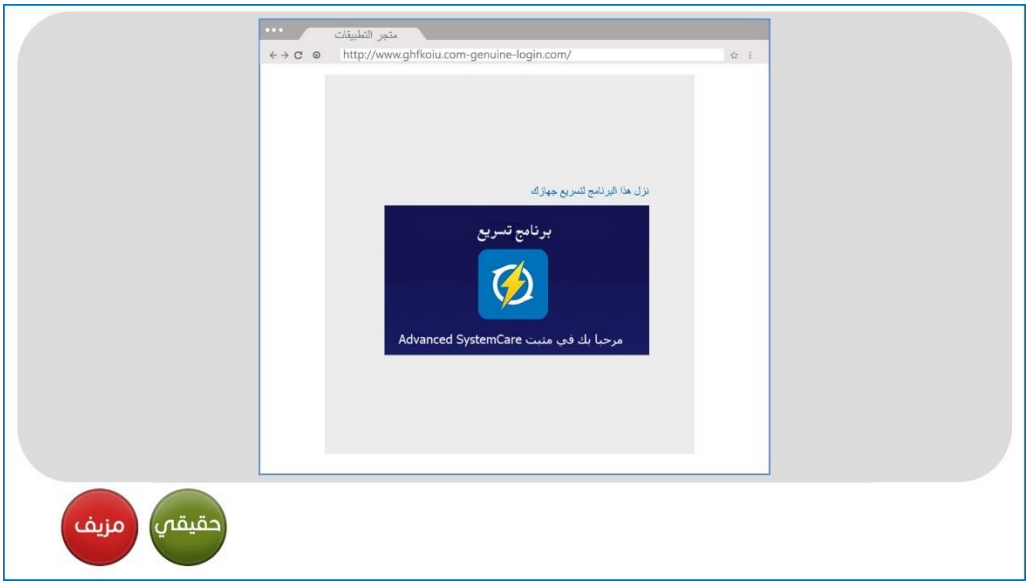
- هل يبدو الموقع مهنيًا مثل مواقع الويب الأخرى التي تعرفها وتثق بها؟ وهل يتضمن شعار المنتج أو الشركة الأصلية، وهل يخلو النّصّ من الأخطاء الاملائية؟
- هل يتوافق عنوان (URL) مع اسم المنتج أو الشركة والمعلومات التي تبحث عنها؟
- هل هناك أي نوافذ منبثقة غير مرغوب فيها؟
- هل يبدأ عنوان URL في :/https ويظهر إلى يساره قفل أخضر صغير؟ (هذا يعني أن الاتصال آمن)
- ماذا يوجد في التفاصيل المطبوعة بخط صغير؟ (تحتوي عادة التفاصيل الخادعة)
- هل يعرض البريد الإلكتروني أو الموقع أمرًا مشبوهًا، مثل فرصة كسب الكثير من المال؟
- هل يساورك شعورٌ غريب تجاه الرسالة؟ كما لو أنّهم يعرفونك، ولكنك لست متأكدًا تمامًا؟

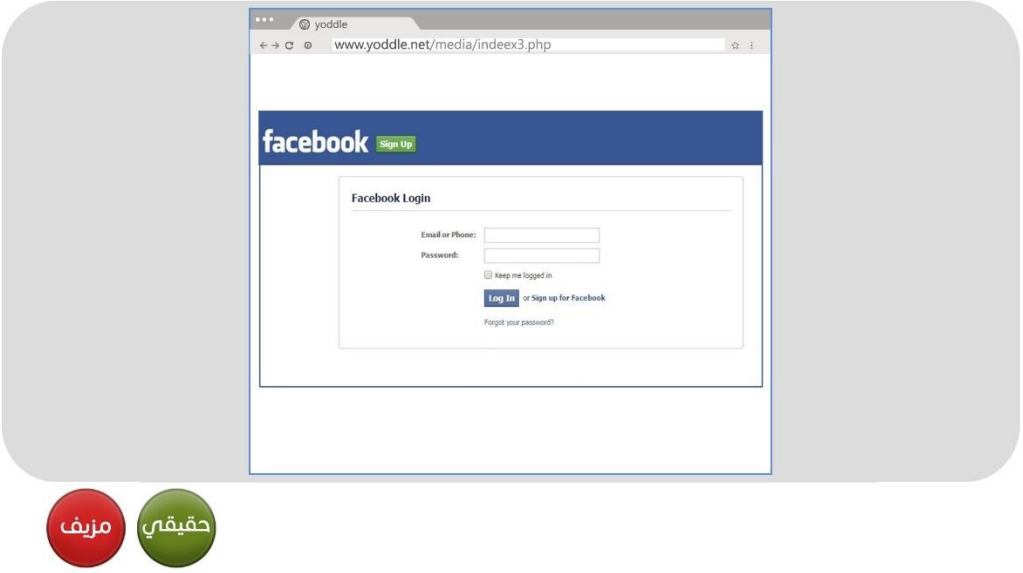
النشاط 2	**مزيف أم حقيقي**
	الفئة العمرية 11–16 عامًا
الهدف	تعزيز توجهات الطلاب في تمييز محاولات التصيّد الاحتيالي والتنبّه لها.
الطريقة	أمثلة لمواقع ورسائل
الأدوات اللازمة	ملف "أمثلة على التصيّد الاحتيالي" يتم توزيعها على الطلاب
التفاصيل	لنتوزع في مجموعات، ولتدرس كل مجموعة هذه الأمثلة عن رسائل ومواقع ويب. حدّد/ي صفة كل مثال "حقيقي" أم "مزيف" واشرح/ي أسباب الخيار. ثم نقوم بنقاش: أيٌّ من الأمثلة بدت جديرة بالثقة وأيّها بدت مشبوهة؟ هل فاجأتك إحدى الإجابات؟ إذا كان الجواب نعم، اشرح السبب. في ما يلي بعض الأسئلة التي تساعدك على تقييم الرسائل والمواقع التي نجدها على الإنترنت: - هل تبدو هذه الرسالة صحيحة؟ - ما هو حدسك الأول؟ هل تلاحظ/ين أيّ أجزاء مشبوهة؟

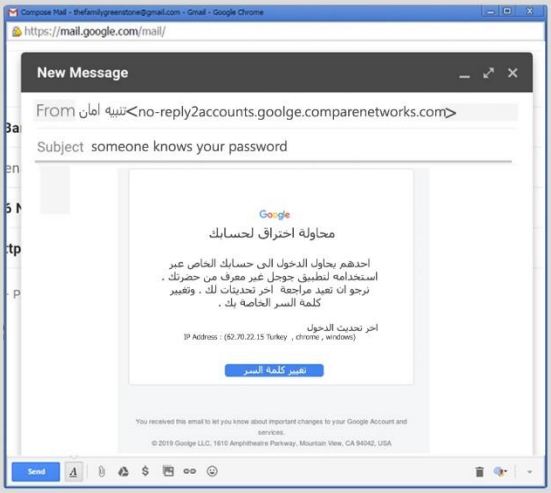
	- هل يُعرض عليك إصلاح مشكلة أنت لا تعرف/ين بوجودها؟ - هل تقدم لك هذه الرسالة عرضًا مغريًا؟ ملاحظة: تكون العروض المجانية غير حقيقية عادة. - هل تطلب معلوماتك الشخصية؟ تطلب بعض مواقع الويب معلوماتك الشخصية حتى تتمكن من إرسال المزيد من محاولات الاحتيال، على سبيل المثال قد تهدف الاختبارات القصيرة أو "الاختبارات الشخصية" إلى جمع الحقائق التي تسهل توقّع كلمة المرور الخاصة بك وأي معلومات عنك، والجدير بالذكر أنّ معظم الشركات الحقيقية لا تطلب معلومات شخصية عبر البريد الإلكتروني. - هل هذه سلسلة بريد إلكتروني أو منشور اجتماعي؟ إن الرسائل الإلكترونية والمشاركات التي تطلب منك إرسالها إلى جميع الأشخاص الذين تعرفهم قد تعرضك أنت والآخرين للخطر، لا تقم/ تقومين بإرسالها إلّا إذا كنت واثقًا/واثقة من المصدر، ومن أنّ الرسالة آمنة. - هل هنالك تفاصيل مكتوبة بخطّ صغير؟ ستجد في أسفل معظم المستندات تفاصيل مكتوبة بخطّ صغير، ويحتوي النصّ غالبًا على معلومات يفترض أن تفوتك، على سبيل المثال: قد يشير العنوان في الأعلى إلى حصولك على هاتف مجاني، ولكن في التفاصيل المكتوبة بخط صغير ستقرأ/ين أنه عليك دفع 200 دولار شهريا لهذه الشركة، وتنبّه/ي إلى أنّ غياب هذه التفاصيل مثيرٌ للشبهات بنفس القدر.
ملاحظات	يمكن عمل النشاط بطريقة أخرى، أو كمكمّل للنشاط السابق بهدف تأكيد المعلومات، أو يمكن اعتبارها مهمّة منزلية. من خلال امتحان التصيّد على الرابط والذي يعرض مجموعة من الرسائل والمواقع، وعليك معرفة إذا كانت حقيقية أو مزيفة. https://phishingquiz.withgoogle.com/?hl=ar يمكن أن يقوم الطلاب بتجربة فحص بعض الروابط باستخدام الموقع التالي:

http://www.ichsany.com/wp-admin/css/nvtex/nvtex/index.php

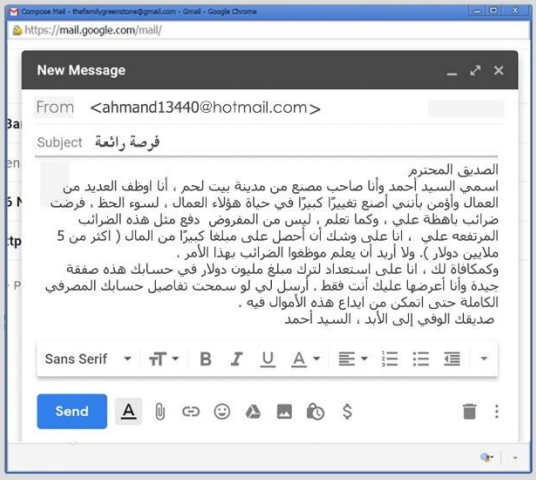
الأمثلة :



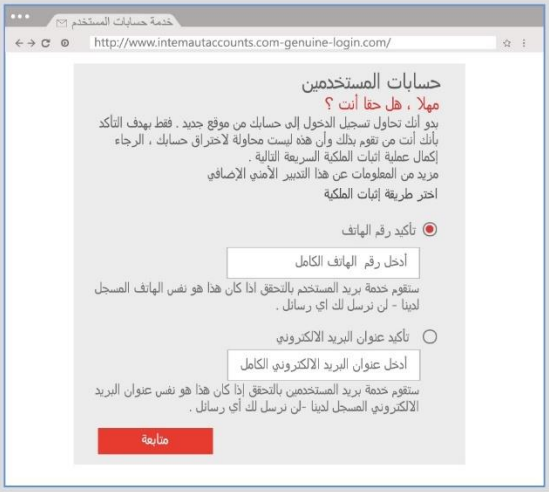




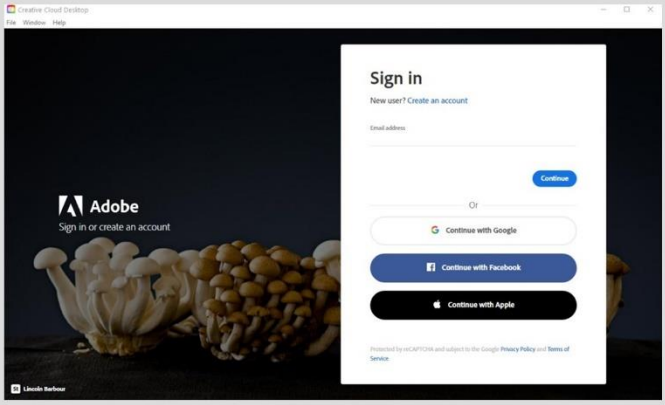
حقيقي مزيف



حقيقي مزيف



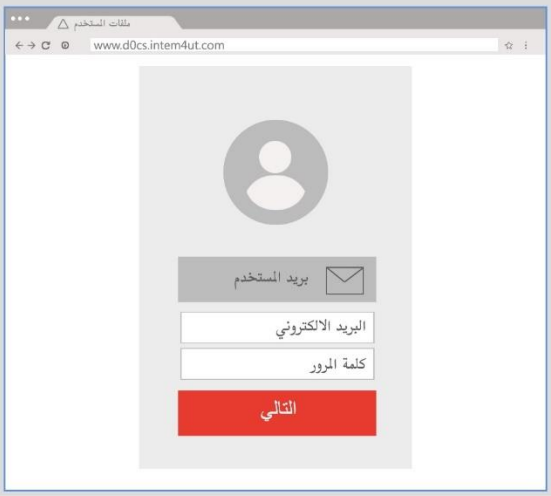
حقيقي مزيف



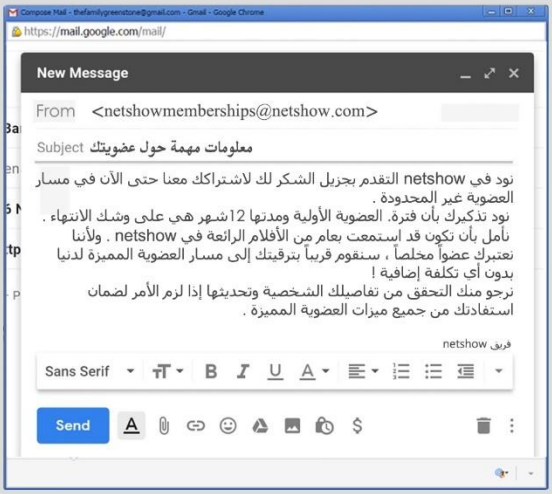
حقيقي مزيف

حقيقي مزيف

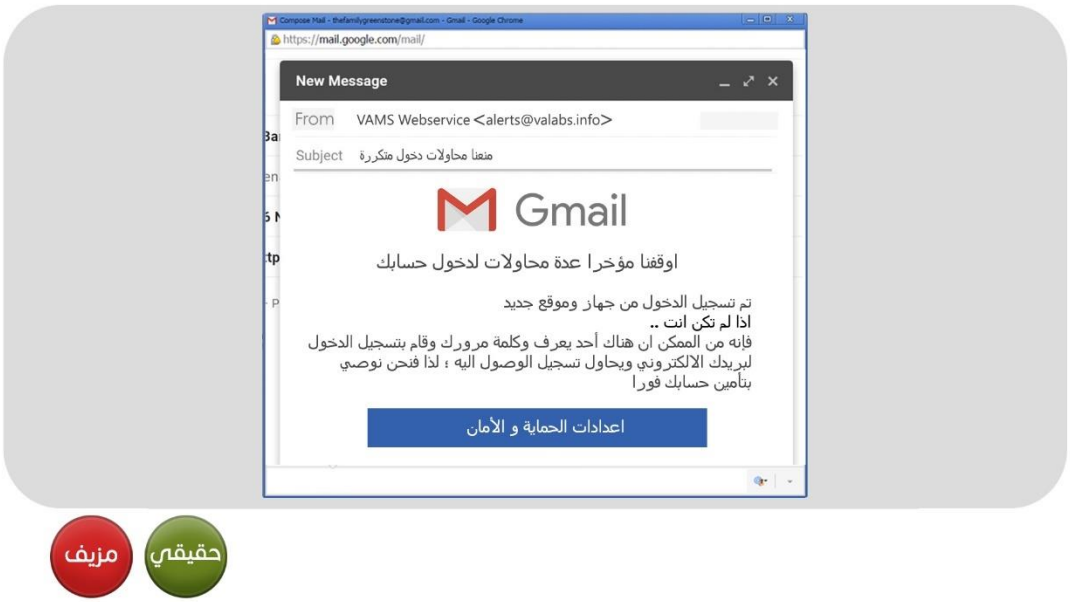
حقيقي مزيف



حقيقي مزيف



حقيقي مزيف

كيف تتأكد من صحة هويتهم؟ عندما تتحدث هاتفيًا مع صديقك، يمكنك التأكّد من هويته من خلال صوته على الرغم من أنّك لا تستطيع رؤيته، ولكن تختلف الأمور في عالم الإنترنت، حيث يصعب أحيانًا التأكد من صحة ادعاءات شخص ما. وفي التطبيقات والألعاب يتظاهر الأشخاص أحيانًا بأنهم أشخاص آخرون على سبيل الدعابة أو بهدف العبث، وفي بعض الحالات ينتحلون صفة أشخاص آخرين بهدف سرقة معلومات شخصية خاصة لإلحاق الأذى بك، وقد يطلب شخصٌ غريبٌ التواصل معك أثناء استخدامك للإنترنت. والأفضل في هذه الحالة عدم الرد، أو إخبار أحد الوالدين أو شخص بالغ تثق به؛ لأنّك لا تعرف الشخص الذي يحاول التواصل معك، وإذا قرّرت الردّ من المستحسن أن تحاول أولًا اكتشاف ما يمكنك معرفته عن الشخص. تحقّق من ملفه الشخصي وقائمة أصدقائه أو ابحث عن معلومات أخرى تؤكد هويته.

هناك طرق متعددة للتحقّق من هوية شخص ما على الإنترنت، وفي ما يلي بعض الأمثلة:

النشاط 3	التحقّق من هوية شخص ما على الإنترنت
الفئة العمرية	11- 16 عامًا

الهدف	تعزيز مهارات الطلبة في مكافحة التصيّد الاحتيالي، والاستجابات المحتملة للنصوص والمشاركات وطلبات الصداقة والصور والرسائل الإلكترونية المشبوهة.
الطريقة	عمل مجموعات، لعب أدوار، عصف ذهني
الأدوات اللازمة	السناريوهات (للفئات العمرية المختلفة)، ورقة الأجوبة للمدرب/ة
التفاصيل	عصف ذهني حول كيف يمكن التحقّق من هوية شخص ما - هل تبدو الصورة في ملفهم الشخصي مشبوهة؟ - هل صورة الملف الشخصي غير واضحة أو يصعب رؤيتها، أو لا يوجد صورة على الإطلاق؟ تسهّل الصور غير الواضحة وصور الحيوانات الأليفة وما شابه ذلك على الشخص بأن يقوم بإخفاء هويته على مواقع التواصل الاجتماعي، ومن الشائع أيضًا سرقة صور شخص حقيقي من أجل عمل حساب مزيف وانتحال هويته, - هل يحتوي الملف الشخصي على اسمهم الحقيقي؟ - هل هنالك معلومات عنهم على ملفهم الشخصي؟ - كم من الوقت مضى على إنشاء الحساب؟ - هل يلائم المحتوى الذي تراه توقعاتك عن الشخص؟ سنتوزع في مجموعات، وستختار كلّ مجموعة سيناريو وتتحدث عن كيفية التصرّف في مثل هذا الموقف. تمثيل السيناريوهات: تقوم كل مجموعة بتمثيل السيناريو الخاص بها مع ردود المجموعة. يتم التأكيد على: أنت تقرر مع من تتحدث على الإنترنت... تأكّد من هوية الأشخاص الذين تتواصل معهم. - **السيناريو الأول**– يصلك طلب صداقة من شخص غريب... "مرحبا، يبدو أنك شخص مرح، دعنا نمضي بعض الوقت الممتع سويًا، أرجوك اقبل طلب الصداقة". سامر: ماذا تفعل؟ "**تتجاهل**" سامر إذا كنت لا تعرفه، ويمكنك ببساطة أن تقرر عدم التحدّث. **أهلا سامر، هل أعرفك؟** إذا كنت غير متأكد اسأل أولًا.

"**تحظر سامر**" إذا قررت بعد أن تأكّدت من هويته حظره، لن تصلك أي رسائل أخرى منه ولن يصله تنبيهًا أنّك قمت بحظره. "**تحقّق من ملف سامر الشخصي**" كن حذرًا! لأنّه من السهل إنشاء ملفات شخصية مزيّفة. تحقق من قائمة الأصدقاء لدى هذا الشخص ودائرة معارفه، وإذا كان بينكما أصدقاء مشتركين، وفي حال لم يكن هناك نشاط على صفحته فهو مؤشر آخر على أنّه غير حقيقي. "**تُضيف سامر إلى قائمة أصدقائك إذا بدا شخصًا حقيقًا**" لا يُنصح بذلك إلا إذا تأكّدت من هويته. "**مشاركة معلومات شخصية معه**" لا تُشارك معلومات شخصية مع أشخاص لا تعرفهم. - **السناريو الثاني**– تصلك رسالة على تطبيق واتساب: "مرحبًا أنا ياسمين، هل تتذكريني" "**تحظر ياسمين**" قد يبدو هذا تصرفًا فظًا إذا كنت تعرفها/تعرفينها فعلًا، ولكن إذا كنت متأكدًا/ة من أنك لم تلتقِ بأي شخص يُدعى ياسمين أو إذا كانت ترسل لك الكثير من الرسائل وتبالغ في المشاركة عن نفسها، يكون من الأفضل حظرها. "**تتجاهل ياسمين**" إذا كنت لا تعرف هذا الشخص، يمكنك ببساطة عدم الردّ. "**أهلاً ياسمين، هل أعرفك؟**" يُعدّ هذا خيارًا آمنًا إذا لم تكن متأكدًا من مقابلتك لها في السابق، وتريد/ين معرفة ذلك من خلال اكتشاف المزيد. "**أنا لا أتذكّرك، ولكن بإمكاننا التحدث**" هذه ليست فكرة جيدة. - **السيناريو الثالث**– تصلك رسالة: "مرحبًا، أحب مشاركتك، أنت شخص ممتع، ويبدو أنّك لاعب ماهر في هذه اللعبة، هل يمكنك إرسال رقمك لي لنتحدث أكثر". "**تتجاهل**" ليس عليك الردّ إذا كنت لا تريد ذلك. "**تحظره**" إذا شعرت بأنّ هذا الشخص مشبوه. **أهلاً، هل أعرفك؟**" إذا لم تكن متأكدًا، الأفضل أن تستفسر قبل إعطاء معلومات شخصية مثل رقم هاتفك. **حسنًا، رقمي هو...**"كلا! حتى لو تحققت من هوية هذا الشخص، لا يُوصى بمشاركة معلومات شخصية على وسائل التواصل الاجتماعي".	

- **السيناريو الرابع**– تصلك رسالة: "مرحبًا... منشوراتك على فيسبوك رائعة يبدو أنّك فتاة مثقفة وجميلة، هل يمكننا التحدّث؟ أريد أن أسألك عن أمر ضروري" "**تتجاهل الطلب**" قد يكون هذا خيار جيد. "**تحظر هذا الشخص**" لا تتردد إذا لم تشعر بالارتياح تجاه هذا الشخص. "**من أنت؟ كيف يمكن أن أساعدك؟**" إذا أردت المساعدة الأفضل أن تستفسر وتتأكد من هوية الشخص، ولا تشارك معلوماتك الشخصية معه. - **السيناريو الخامس**– تصلك رسالة: "لقد رأيتكِ في المدرسة اليوم، أنتِ جميلة للغاية، يمكننا الدردشة أكثر سويًا" "**تتجاهل الطلب**" قد يكون هذا خيار جيد. "**تحظر هذا الشخص**" لا تتردد إذا لم تشعر بالارتياح تجاه هذا الشخص. "**من أنت؟**" إذا لم تكن متأكدًا، الأفضل أن تستفسر. "**هل هذه أنتِ؟ أنتِ جميلة أيضًا! لا مانع لي لنتحدث**" هذه ليست فكرة جيدة، حتى لو كنتِ تعتقدين أنّكِ تعرفين مرسلة الرسالة، واحذري أن تعطي عنوانك أو أي معلومات شخصية أخرى لأيّ شخص، تحققي من هويته/ها حتى لو كنتِ تعتقدين بأنّك تعرفينه/ها، لا تلتقِ بشخص لمجرّد أنك تعرفينه فقط من خلال التواصل على الإنترنت. - **السناريو السادس**– تصلك رسالة: "مرحبًا، التقيت صديقتك زينة اليوم، حدثتني عنك كثيرًا، وأحببتُ أن أتعرف عليك أكثر". "**تتجاهل/ين الرسالة**" إذا لم يسبق لك معرفة هذا الشخص، ولكن لديك صديقة تدعى زينة، وأفضل ما يمكن فعله هو التحقّق من زينة أولاً قبل الرد على هذه الرسالة. "**تحظر المُرسِل**" إذا لم تكن تعرف هذا الشخص وليس لديك صديقة تدعى زينة، من الأفضل حظر هذا الشخص من خلال الإعدادات لمنعه من الاستمرار في التواصل معك.	

	"من أنت؟" هذه ليست فكرة جيدة إذا لم يسبق لك معرفة هذا الشخص، من الأفضل عدم الرد، على الأقل حتى تستفسري من زينة.
ملاحظات	

"السلامة خيرٌ من النّدامة"

تسهل التكنولوجيا الرقمية عملية التواصل مع الأصدقاء وزملاء الدراسة والمعلمين والأقارب. فيمكننا التواصل معهم بطرق عدة، مثل البريد الإلكتروني والرسائل النصية، والرسائل الفورية، وباستخدام الكلمات والصور والفيديوهات، وعبر الهواتف والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة. (كيف تتواصل/ين مع أصدقائك؟)

لكنْ، تُسهّل نفس هذه الأدوات التي نتبادل فيها المعلومات على المخترقين والمحتالين سرقة تلك المعلومات، واستخدامها لإلحاق الضرر بأجهزتنا وعلاقاتنا وسمعتنا، وعندما معرفة أننا حين نرغب في حماية شيء فإننا نقفله بمفتاح: المنازل والخزنات، والسيارات... كلها لها مفاتيح وأقفال.

حماية أنفسنا ومعلوماتنا وأجهزتنا تعني اتخاذ تدابير ذكية بسيطة، مثل استخدام أقفال الشاشة على الهواتف، وعدم وضع معلومات شخصية على أجهزة غير مقفلة، قد نفقدها أو تتم سرقتها، والأهم من كل ذلك، إنشاء كلمات مرور قوية.

النشاط 4	كلمة المرور القوية
الفئة العمرية	11 –16 عامًا
الهدف	تعزيز معارف الطلاب/ات حول كلمات السرّ القويّة
الطريقة	عصف ذهني

الأدوات اللازمة	لوح، أقلام
التفاصيل	من يستطيع أن يخمّن كلمات السر الأكثر استخداما؟ (الجواب "Password" " و "123456") دعونا نتحدث عن بعض كلمات المرور الأخرى غير المناسبة، وما الذي يجعلها غير مناسبة: اسمك الكامل، ورقم هاتفك، وتاريخ ميلادك، إلخ... من يعتقد أن كلمات المرور هذه جيدة؟ متى تكون كلمة المرور قويّة؟ عرض جدول بأكثر كلمات السر الشائعة لعام 2019 Top 20 most common passwords according to NCSC

Rank	2019[14]
1	123456
2	123456789
3	qwerty
4	password
5	1111111
6	12345678
7	abc123

	1234567	8	
	password1	9	
	12345	10	
	1234567890	11	
	123123	12	
	000000	13	
	Iloveyou	14	
	1234	15	
	1q2w3e4r5t	16	
	Qwertyuiop	17	
	123	18	
	Monkey	19	
	Dragon	20	
ملاحظات	ممكن من خلال هذا الموقع الوصول لكلمات السر الشائعة المحدثة باستمرار https://nordpass.com/most-common-passwords-list/?utm_medium=affiliate&utm_term&utm_content=100031977&utm_campaign=off490&utm_source=aff34741&aff_free		

متى تكون كلمة المرور قويّة؟

- عندما تكون طويلة: كلما كانت كلمة المرور أطول، قلّ احتمال تخمينها من قبل برامج الحاسوب في مدة زمنية قصيرة.
- عندما تكون معقّدة: إضافة إلى طول كلمة المرور، يساعد التعقيد على منع برمجيات "كسر كلمة المرور" التلقائية من تخمين التركيب الصحيح لحروف الكلمة، وينبغي أن تتضمن كلمةُ المرور حروفًا صغيرة، وحروفًا كبيرة، وأرقامًا، ورموزًا– كلما كان ذلك ممكنًا–.
- عندما لا تكون شخصيّة: لا يجب أن تكون كلمة مرورك مرتبطة بشخصيّتك. لا تختزْ/تختاري كلمةً أو عبارةً تعتمد على معلومات مثل: اسمك أو يوم ميلادك، أو رقم هاتفك، واسم طفلك، واسم حيوانك الأليف، أو أيّ معلومة يمكن لشخصٍ ما أن يعرفها عنك بقليل من البحث.
- عندما تكون سرّية: لا تشارك/ي كلمة مرورك مع الآخرين، إلّا إذا كان ذلك محتّمًا عليك.
- عندما تكون فريدة: تجنّب استخدام كلمة المرور ذاتها لأكثر من حساب واحد، وإلّا فإنّ كشفها سيتيح الوصول لخدماتٍ إضافية، وللمعلومات التي تحتويها هذه الخدمات.
- عندما تبقى محدّثة: غيّر كلمات مرور حساباتك الهامة دوريًا، وكلما طالت فترة استخدامك لكلمة المرور زادت فرصة كشفها من قبل الآخرين، وإن حدث ذلك فإنّهم سيستمرون باستخدامها للولوج إلى حساباتك دون علمك إلى أن تُغيّرها. كلما كانت كلمة مرورك قويّة– حسب المعايير الموضّحة أعلاه– قلّت الحاجة لتبديلها باستمرار. لكن يبقى من الجيّد أن تُحدّث/ين كلمات مرورك سنويًا أو نحو ذلك.

يُعدُّ اختيار كلمة مرور قوية وفريدة لكلّ حسابٍ من حساباتك المهمة خطوة أولى رائعة، أمّا الخطوة الثانية فهي تذكّر كلمات المرور الخاصة بك والاحتفاظ بها فقط لنفسك.

النشاط 5	كلمة المرور الأقوى
الفئة العمرية	11 –16 عامًا

الهدف	تعزيز مهارات الطلاب/ات في إنشاء كلمات سرّ قوية.
الطريقة	مسابقة
الأدوات اللازمة	أوراق، لوح، أقلام
التفاصيل	إنشاء كلمات مرور لنتوزع في فرق مكونة من شخصيْن، لدى كل فريق دقيقة لإنشاء كلمات مرور قوية. سيقوم فريقان في كل مرة بالتزامن بكتابة كلمة المرور الخاصّة بهما على اللوح. يتم التصويت على كل زوج من كلمات المرور ومناقشة أيّها أقوى. ثم مناقشة...
ملاحظات	من الممكن استخدام الرابط التالي لجعل الطلاب يقومون بتجربة فحص بعض كلمات المرور ومدى قوتها. افحص/ي قوة كلمة السر http://www.passwordmeter.com ملاحظة: من المهم تذكير الطلبة بأن لا يكتبوا كلمة سرّ بعينها، وإنما شبيه لها من حيث المبنى.

بعد تعيين كلمات مرور قوية لجميع حساباتك، نأتي الآن إلى الخطوة التي تليها أهميةً لحماية هذه الحسابات، وهي تفعيل التحقق بخطوتين، يرمز له اختصارًا بـ "2FA"، ويعني أنه بالإضافة إلى كلمة المرور، ستحتاج إلى تقديم معلومة ثانية لتسجيل الدخول.

ما هي المصادقة الثنائية (التحقق بخطوتين) Two-factor authentication؟

هي ميزة أمان تساعد على حماية حسابك، بالإضافة إلى كلمة المرور الخاصة بك، وإذا قمت بتفعيل المصادقة الثنائية، فسيُطلب منك إدخال رمز تسجيل دخول خاص، أو تأكيد محاولة تسجيل الدخول الخاصة بك في كل مرة يحاول شخص ما الوصول إلى حسابك من متصفح أو جهاز محمول لا نتعرف عليه. يمكنك أيضًا الحصول على تنبيهات عندما يحاول شخص ما تسجيل الدخول من متصفح أو جهاز محمول لا نتعرف عليه.

عندما تقوم بتسجيل الدخول إلى حساب عبر الإنترنت باستخدام اسم مستخدم وكلمة مرور، فإنّك تستخدم ما يسمى المصادقة الأحادية، وتحتاج فقط إلى شيء واحد للتحقق من شخصيتك، وهي كلمة المرور فقط.

مع 2FA تحتاج إلى توفير شيئيْن: كلمة المرور الخاصة بك، وشيء آخر مثل الرمز الذي يتم إرساله إلى جهازك المحمول أو بصمة إصبعك حتى تتمكن من الوصول إلى حسابك.

ستطالبك بعض الخدمات عبر الإنترنت تلقائيًا بعامل ثانٍ عند تسجيل الدخول، ومع ذلك فإنّ العديد من الخدمات لا تطالب بذلك، لذا ستحتاج إلى تفعيله بنفسك، وستجد خيار تشغيل 2FA في إعدادات الأمان أو الخصوصية لحساباتك عبر الإنترنت.

النشاط 6	**المصادقة الثنائية، أو التحقق بخطوتين**
الفئة العمرية	11- 16 عامًا
الهدف	تعزيز مهارات الطلاب/ات وتوجهاتهم حول أهمية المصادقة الثنائية.
الطريقة	لعبة "حارس الأمن المزعج".
الأدوات اللازمة	
التفاصيل	شخص في موقف يُفترض أن يُسمح له بالدخول إلى حفلة أو حدث ما، ولكن هناك حارس أمن مسؤول لا يصدقه؟ اختر شخصًا ليكون "حارس الأمن المزعج"، أو إذا كان لديك مجموعة صغيرة، شجع الجميع على أن يكونوا "الحارس". يجب محاولة اقناع الحارس لكي يسمح له بالدخول "مرحبًا... اسمي XXX ، وقد جئت إلى هنا للمشاركة في الحفل، هل تجد اسمي في القائمة؟" يجب أن يختلق الحارس سببًا للمنع مثل "لا أرى اسمك" أو "كيف أعرف أنه أنت حقًا؟"

على الشخص محاولة اثبات هويته للحارس "حسنًا... ها هي بطاقة هويتي، هناك صورة لي"، أو "اسأل إذا كان هنالك شخص يعرفني في الداخل"، أو "هذه صورة لي على Instagram مع صاحب الحفل"... وما إلى ذلك. ما يُظهره هذا هو أنّه لا توجد طريقة واحدة مثالية لإثبات هويتك، ولكن كلما زادت الطرق التي يمكنك من خلالها إثبات هويتك، زادت احتمالية أن يكون التعريف صحيحًا وحقيقيًا. حارس الأمن ليس مخطئًا في التشكيك بإثبات الهوية. وفي النهاية عليه أن يُثبت عذا الرجل أنه الشخص الحقيقي، وليس شخصًا آخر يدّعي أنّه هو. بمجرد الانتهاء من نشاط "حارس الأمن المزعج"، اشرح/ي كيف يرتبط هذا بالنشاط: "الآن قم/قومي بتطبيق هذا على تسجيل الدخول إلى أيّ حساب. وليكن معلومًا أن معظم عمليات تسجيل الدخول تطلب فقط من المستخدمين إثبات هويتهم بطريقة واحدة: – كلمات المرور: المشكلة في كلمات المرور هي أن شخصًا آخر قد يحصل عليها. هذا ما سيقوله حارس الأمن المزعج. ربما رأيتم من قبل آلية استخدام ماكينة الصراف الآلي: تحتاج إلى كل من رقم التعريف الشخصي وبطاقتك للسماح لك بالسحب أو إيداع الأموال. ويمكن لشخص آخر معرفة رقم التعريف الشخصي الخاص بك أو يمكنه سرقة بطاقتك، ولكن من غير المرجّح أن يتمكنوا من القيام بالأمريْن معًا. لذا فإن "العامل الثنائي" يعني شيئًا آخر بخلاف كلمة المرور، بالإضافة إلى كلمة المرور. وتُعتبر كلمة المرور الخاصة بك بمثابة "عامل" التعريف الأول، وبعد ذلك تحتاج إلى تقديم واحدٍ آخر للسماح لك بالدخول.	

ملاحظات	لفت انتباه الطلاب أنّ المصادقة الثنائية مثل أي إجراء آخر له إيجابيات وسلبيات. فهو إيجابي من حيث قوة الحماية، وسلبي من حيث الراحة في الاستخدام.

النشاط 7	تفعيل المصادقة الثنائية
الفئة العمرية	11- 16 عامًا
الهدف	تعزيز مهارات الطلاب حول كيفية تفعيل خاصية المصادقة الثنائية على بعض المواقع.
الطريقة	عرض توضيحي
الأدوات اللازمة	حاسوب، بروجكتر
التفاصيل	يقوم المدرب بتوضيح أن أغلب التطبيقات والخدمات على الإنترنت توفّر خاصية المصادقة الثنائية، ومنها: "فيسبوك، انستغرام، سناب شات، واتساب، جيميل، تويتير" ثم يقوم بعرضٍ عمليّ لكيفية تفعيلها على أحد المواقع، ثم يطلب من الطلاب محاولة تفعيلها على مواقع أخرى، أو يطلب من الطلاب الذين سبق لهم تفعيلها بشرح الخطوات للآخرين.
ملاحظات	أدلّة حول كيفية تفعيل المصادقة الثنائية/ التحقّق بخطوتيْن على بعض المواقع دليل التحقق بخطوتيْن على فيسبوك https://digital-protection.tech/2018/06/01/facebook/ دليل التحقق بخطوتين على جيميل https://digital-protection.tech/2018/06/01/gmail/ دليل التحقق بخطوتين على الانستقرام https://digital-protection.tech/2018/06/01/instagram

10نصائح للحفاظ على أمنك الرقمي على الإنترنت:

1- تحديث البرامج وأنظمة التشغيل باستمرار

يقوم مُعظم مُصنّعي البرامج بشكل دوري بإصدار تحديثات لمعالجة مشكلات أمان محددة. وتُعتبر الأجهزة القديمة أكثر عرضة للتعطل وللثغرات الأمنية وللهجمات الإلكترونية من تلك التي يتم تحديثها update باستمرار. وعلى الرغم من ذلك، يتجاهل العديد من الأشخاص المطالبات لتحديث البرامج. حيث إنّ تحديث أنظمة التشغيل و البرامج بشكل دوري يوفّر لنا الحماية من البرمجيات الخبيثة.

2- استخادم كلمات سر قوية وفريدة

3- استخدام مضاد فيروسات

هناك العشرات من خيارات برامج مكافحة الفيروسات المجانية التي تحمي كل جميع الاجهزة. مثل Avg – Malwarebytes، ويجب استخدام مضاد فيروسات واحد فقط على نفس الجهاز.

4- تفعيل المصادقة الثنائية

5- تأكد من الرابط قبل الضغط عليه.

6- التصفح باستخادم https:// قدر الإمكان.

7- تقليل مشاركة المعلومات الشخصية قدر الإمكان.

8- تجاهل الحديث المثير للشك والفضول قدر الإمكان.

9- تحميل البرامج من المتاجر الرسمية على الهواتف الذكية أو من مواقعها الرسمية فقط.

10- هناك الكثير من الروابط التي تنتشر على الشبكات الاجتماعية مثل "اعرف مين زار بروفايلك" وغيرها من والوسائل والتطبيقات الوهمية التي قد تلحق الأذى بك.

*نشاط للمراجعة

النشاط 8	**الحصن**

الفئة العمرية	11-16 عامًا
الهدف	تعزيز معارف الطلاب/الطالبات حول آليات وإجراءات زيادة الأمان والحماية على الإنترنت
الطريقة	صندوق المجموعات/ عمل مجموعات
الأدوات اللازمة	صندوق، أوراق الحصن، ورق كبير
التفاصيل	يوجد في الصندوق ورقة فيها نصيحة لزيادة الأمان على الإنترنت، على المجموعات سحب ورقة ونقاشها داخل المجموعة، ومن ثم عرض المخرجات على الزملاء في الصف. يمكن بناء الحصن من خلال الأدوات التي نجدها مع الورقة. يمكن استخدام أدوات الرسم أو أدوات ليجو لبناء الحصن بعد شرح كل بعد من الأبعاد.
ملاحظات	يمكن إضافة أي نصائح أخرى تم ذكرها خلال الدليل

المواقف التي تستدعي المساعدة (متى نطلب المساعدة) وما هي آلية الإبلاغ؟

من المهم أن يدرك الطلبة بأنهم ليسوا وحدهم عندما يرون محتوىً على الانترنت يشعرهم بعدم الارتياح، وخاصة إذا شعروا أن ذلك قد يعرضهم وأشخاصًا آخرين للأذى، يجب ألّا يتردّدوا أبدًا في طلب المساعدة من شخص يثقون به، ومن الجيّد أيضًا أن يعرفوا أن هناك طرقًا مختلفة للتصرّف واتخاذ الخطوات، بدءًا من التحدّث عن الأمور في الواقع، وصولًا للإبلاغ عبر الإنترنت.

من النصائح التي تتكرر خلال هذه الأنشطة هي: إذا صادف الطلبة أمرًا يجعلهم يشعرون بالقلق أو ما هو أسوأ من ذلك، أن نشجّعهم على الإبلاغ عنه، وأن يتحلّوْا يالشجاعة ويتحدثوا مع شخص يثقون به للمساعدة، بما في ذلك أنت أو أحد الوالديْن في حال تعرضت للمضايقة عبر الإنترنت.

إذا تعرضت لأيّ سلوك مسيء على الإنترنت، إليك بعض الأمور التي يمكنك القيام بها:

- عدم الرد.
- حظر الشخص.
- إخبار أحد الوالديْن أو المرشد التربوي، أو أي شخص آخر يمكن الوثوق به.
- استخدام أدوات الإبلاغ في التطبيق أو الخدمة.

ملاحظات مهمّة للمدرّب:

–لقد تم تعليم الأطفال و المراهقين/ات أو تهيئتهم لِما يُسمى "عدم الوشاية" على مدى عدة أجيال، لدرجة أنّ هذا الأمر قد تحوّل إلى معيار اجتماعي، وهنا يجب العمل على فهم الفرق بين "الوشاية" وطلب المساعدة.

– ساعد طلبتك على الفهم بأنّ طلب الدعم عند تعرّضهم لمواقف مؤذية على الإنترنت لا يعتبر "وشاية"؛ بل يتعلق بطلب المساعدة لأنفسهم أو لأقرانهم عند التعرض للأذى.

–يساهم تعزيز التواصل المفتوح في الصفّ وتذكير الطلبة بأنّك موجود دائمًا لدعمهم في زيادة إحساسهم بالّراحة والمسؤولية، وتشجيعهم على الإبلاغ في الحالات المناسبة.

–في المناقشة أدناه، في كلِّ مرّة يشارك فيها الطلبة أمثلةً على مواقف طلبوا فيها المساعدة من شخص بالغ، التأكد من أنّهم يتحدثون بنبرة تنمُّ عن شعور بالفخر والشجاعة لقيامهم بذلك، وخاصة أنّهم يتحدثون أمام أقرانهم.

النشاط 1	**مواقف تستدعي طلب المساعدة**
الفئة العمرية	11–16 عامًا
الهدف	تعزيز معارف وتوجهات الطلاب/ات في المواقف التي قد تستدعي طلب المساعدة، أو التحدث مع شخصٍ بالغٍ موثوقٍ به حول الخيارات المتاحة للتصرف بشجاعة، والإدراك بأنّ طلب المساعدة لأنفسهم أو للأخرين هو دليل على القوّة.
الطريقة	نقاش فعال
الأدوات اللازمة	قائمة المواقف

التفاصيل	فيما يلي قائمة من المواقف التي قد تصادفها على الإنترنت، قد لا تناقشها جميعها ولكنني أتمنّى أن ترفعوا أيديكم عندما يُذكّركم أحد المواقف الواردة في القائمة بحالة مررتم بها وكيف تصرفتم حيالها وذلك حين نتمكن من التحدث عن هذه الحالات معًا. **أمثلة على المواقف:** - كان لديك شعورٌ أنّ حسابك تعرّض للاختراق والسرقة. - نسيت كلمة السر. - لم تكن متأكدًا إذا ما كان أمرٌ معينٌ مثل احتيال... أو إذا وقعت فعلًا ضحية لمحاولة احتيال. - حاولَ أحدُ الأشخاص مناقشة موضوعٍ معك جعلك تشعر بعدم الارتياح. - وصلتك رسالةٌ أو تعليقٌ مريبٌ من شخصٍ غريبٍ. - شعرت بالقلق لأنك شاركت شيئًا على الإنترنت لم يكن ينبغي أن تشاركه. - أحدهم يُصرّ على ملاحقتك على الإنترنت، وإرسال طلبات صداقة لك باستمرار. - كنتِ قلقةً بشأن رسائل ترسلها صديقتك لبعض الأشخاص. - أرسل أحدهم لك محتوىً غيرَ لائقٍ. قراءة القائمة بصمت!... أثناء ذلك فكّروا إذا ما كنتم قد واجهتم أحد هذه المواقف، وهل فكّرتم في طلب المساعدة من شخصٍ بالغٍ في أيٍّ منها؟ وهل طلبتم المساعدة فعًلا؟ ارفع/ي يدك إذا كنت تريد/ين إخبارنا بما فعلته (أو لم تفعله/تفعليه) ولماذا؟ إذا اختار الشخص أحد المواقف، يمكنك اختيار موقف ملائم آخر للحديث عنه. دعونا نناقش هذه المواقف...

ملاحظات	قاعدةٌ تنطبق على جميع أنواع التواصل الرقمي: يجب أن يشعر الأطفال بالأمان والراحة في التحدّث إلى شخصٍ بالغٍ يثقون به إذا صادفوا محتوًى مشبوهًا على الإنترنت، ويمكن للبالغين دعم هذا النوع من التواصل من خلال توفير بيئات حاضنة ومفتوحة في المنزل والمدرسة.

النشاط 2	**خط الدفاع**
الفئة العمرية	11–13 عامًا
الهدف	تعزيز توجّهات الطلبة بالتوجّه للأهل والمقرّبين لطلب المساعدة
الطريقة	لعبة خط الدفاع
الأدوات اللازمة	أوراق، أقلام.
التفاصيل	يتم توزيع أوراقٍ فارغةٍ على الطلاب والطلاب، ويُطلب منهم أن يكتبوا من هو الشخص الذي يمكن أن يتوجهوا إليه لحل المشكلة، ولماذا هذا الشخص تحديدًا؟ يتم نقاش الاستجابات وعمل عصف ذهني عليها.
ملاحظات	

تحتوي معظم التطبيقات والخدمات على أدوات للإبلاغ عن المحتوى غير اللائق أو حظره، ويمكن للأشخاص المعنيّين والمنصّات نفسها الاستفادة من استخدامنا لهذه الأدوات، وتذكّر! قبل حظر المحتوى غير اللائق أو الإبلاغ عنه، من المفيد دائمًا حفظ لقطة شاشة حتى يكون لديك توثيقًا للمواقف.

عندما يظهر محتوى فظٌّ وغيرُ لائق على الإنترنت، فإنّ لدى الأشخاص عدة خيارات للتصرف حياله، وقد ناقشنا في النشاط السابق أهم الخيارات؛ ألا وهو التحدّث مع شخص تثق به، كما إنه لديك خيارٌ آخر وهو الإبلاغ عنه للتطبيق أو الخدمة، والذي قد يساعد على حذفه... من المهم الاعتياد على استخدام أدوات الإبلاغ على الإنترنت.

يجب ان يعتاد الطلاب على أخذ لقطة الشاشة من المحادثات أو النشاط الضارّ قبل استخدام أداة الحظر والابلاغ، وبالتالي لا نستطيع توثيق النشاط السيء، هذا يضمن بأن يتمكن البالغون من تصديقهم والمساعدة في إيجاد حلّ.

يشير المدرب إلى أنّ الجميع قد يخطئ، فإذا فعلت أو تبادلت شيئا ندمت عليه، فلا تدع الإحراج يمنعك من الإبلاغ عن حالة ربما تُسبب خطرًا أو تهديدًا.

يعتمد المحتالون في بعض الحالات على العار الذي يشعر به الضحايا لطلب المزيد من الصور أو مقاطع الفيديو أو المعلومات الشخصية، وإذا كنت هدفًا للابتزاز أو التهديد، أوقف أيّ اتصال مع الشخص المحتال.

النشاط 3	الإبلاغ عبر الإنترنت
الفئة العمرية	11–16 عامًا
الهدف	تعزيز معارف الطلاب وتوجّهاتهم حول استخدام أدوات التبليغ عن الإساءة.
الطريقة	عرض
الأدوات اللازمة	أجهزة حاسوب
التفاصيل	احصل على أكبر عدد ممكن من الأجهزة التي يمكن لصفك الوصول اليها، إذا كان هناك عدة أجهزة، قسّم الصفّ إلى مجموعات، وابحثوا معًا عن الأدوات في ثلاثة حسابات على الأقل للابلاغ عن محتوى سيء أو سلوكٍ غير لائق، أمّا إذا كان هناك جهاز "كمبيوتر" واحد فقط في الغرفة فإنّه يمكن أن تتناوب مجموعات الطلبة على استخدام الجهاز.
ملاحظات	

النشاط 4	هل ستبلغ عن هذ المحتوى؟
الفئة العمرية	11 –16 عامًا
الهدف	تعزيز معارف ومهارات الطلبة في الحالات التي يجب فيها التبليغ عن إساءة.
الأدوات اللازمة	سيناريوهات (لفئات عمرية مختلفة)
التفاصيل	الاطّلاع على السيناريوهات: يجب على كلّ الطلبة في الصفّ الاطّلاع على المواقف المذكورة: هل ستبلغ عن هذا المحتوى؟ اطلب/ي من الطلبة رفع أيديهم إذا كانوا سيبلغون عن المحتوى، ثم اطلب منهم رفع أيديهم إذا كانوا لن يبلغوا عن ذلك. إذا كان الجوال نعم، لماذا؟ اطلب/ي من طالب/ة قد يبلغ/تُبلغ عن المحتوى أن يشارك/تشارك السبب مع الصف، واطلب/ي من طالب/ة لن يقوم بالتبليغ عن المحتوى شرح أسبابه/ها. **أمثلة على المواقف:** **الموقف الأول:** أنشأ طالبٌ حسابًا لطالب تعرفه مُستخدمًا اسم هذا الطالب وصورته الشخصية، كما حوّل الصورة إلى مشاركة مضحكة من خلال رسمِ شاربٍ وملامحِ وجهٍ غريبةٍ عليها، بحيث تحوّلت الصورة إلى مزحة، هل ستبلغ عن هذا الحساب؟ **الموقف الثاني:** خلال مشاهدتك لفيديو على الإنترنت يظهر فيه محتوى غير لائق ويُشعرك بعدم الارتياح، هل تبلغ عنه أم لا؟ **الموقف الثالث:** خلال ممارستك للعبة على الإنترنت مع أصدقائك بدأ أحد الأشخاص الذين لا يعرفهم أيّ من اللاعبين بالدردشة معك، مع أنّه لم يزعجك بأيّ شكل من الأشكال، ولكنّك لا تعرفه. هل تتجاهله أم تبلّغ عنه؟

	الموقف الرابع: يرسل أحدُهم لك صورًا ونكاتٍ غيرَ لطيفةٍ، هل تبلغ عنه أم لا؟ **الموقف الخامس:** قام أحد الطلاب بنشر صورة جماعية في حساب عام، وأنتَ غيرُ راضٍ عن مظهرك في هذه الصورة. هل تبلّغ عن هذه الصورة أم لا؟ كيف يمكنك التعامل في مثل هذا الموقف؟ **الموقف السادس:** إذا لاحظتَ أنّ طالباً علّق على الإنترنت قائلًا: إنّه سيتشاجر مع طالبٍ آخر في المدرسة في اليوم التالي، هل تبلّغ عن هذا التعليق؟ على الإنترنت أم لا؟ وهل تُبلّغ عنه إلى المعلم أو المدير في صباح اليوم التالي أم لا؟ أو هل تبلغ عن التعليق بالطريقتيْن؟
ملاحظات	يجب أنْ يدركَ الجميعُ بأنّه نادرًا ما يكون هناك اختيارٌ واحدٌ صحيح بالمطلق، وهذا ما يجعل المناقشة مفيدة، كما لا ينبغي لأحدٍ أن يشعر بالسوء إزاء خياره. فالبالغون أيضًا لا يعرفون دائمًا متى أو كيف يجب الإبلاغ.

مساعدة الآخرين

يخلق العالم الرقمي تحدياتٍ وفرصًا جديدةً للتفاعل الاجتماعي لجميع المستخدمين/ات، وقد يصعب قراءة الإشارات الاجتماعية على الإنترنت، وقد يسبب التواصل المستمر الراحة والقلق على حدٍّ سواء، كما يمكن أن يؤديَ إخفاء الهوية إلى زيادة الإعجاب والمجاملات، بالإضافة إلى إلحاق الأذى بالذّات والآخرين.

هذا الأمر معقدٌ بعض الشيء؛ ولكنّنا نعلم بأنّ للإنترنت قدرة على زيادة تأثير اللطافة أو السلبيّة على حدٍّ سواء، ومن الضروري تعلّم كيفية التعبير بلطف وتعاطف، وكيفية الاستجابة للسلبية والمضايقة من أجل بناءِ علاقات صحية، وكذلك من أجل الحدِّ من مشاعر العزلة التي تؤدي في بعض الأحيان إلى التنمّر والاكتئاب وصعوبات التعلم وغيرها من المشاكل.

تُشير الأبحاث إلى أنه بدلًا من نهي الأطفال عن التصرف بسلبيّة على الإنترنت، يجب التحدّث عن سبل الحدِّ من التنمّر لمعالجة الأسباب الكامنة وراء السلوك السلبي، وتشجع هذه الأنشطة مع الطلبة لإحداث التفاعل بشكل إيجابي من البداية، وتعليمهم كيفية التعامل مع السلبية عند ظهورها.

إذا كنت شاهدًا على حدوث مضايقة أو تنمّر، لديك خيار التدخل والإبلاغ عن السلوك المسيء، وفي بعض الأحيان لا يحاول المتفرجون إيقاف التنمر أو مساعدة الشخص المستهدف، ولكنْ عندما يفعلون ذلك فهم يتحولون إلى مدافعين، ولذلك يمكنك الاختيار بين أن تكون مدافعًا من خلال اتخاذ قرار بعدم دعم السلوك الفظّ والدفاع عن اللطافة والايجابية، وقد يكون للقليل من الإيجابية صدى كبير على الإنترنت، فهي قد تمنع انتشار السلبيّة وتحولّها إلى سلوكيات قاسية ومؤذية,

أهم ما يجب معرفته هو أنّه بالإمكان مساعدة الشخص المستهدف بمجرد مواساته وجعله يشعر بأنّ هنالك من يهتمّ لأمره.

قد لا يشعر الجميع بالراحة في مواجهة الآخرين **علنًا**، سواء على الإنترنت أو المدرسة.

إذا كنت مستعدًا لذلك، لا تتردد! بإمكانك فعل الكثير:

- انتقاد السلوك الفظ، وليس الشخص **أو** وصفه بأنّه غير لطيف.
- قول أمرٍ لطيفٍ عن الشخص المستهدف في مشاركة أو تعليق.
- الطلب من أصدقائك كتابة تعليقات لطيفة عن الشخص المستهدف على الإنترنت أيضًا.
- في العالم الفعلي، يمكنك دعوة الشخص لقضاء الوقت معك.

لا بأس إذا كنت لا تشعر بالراحة لتقديم الدعم له علنًا، يمكنك أيضًا دعم الشخص المستهدف **بشكل غير علني**. بإمكانك:

- السؤال عن أحواله في رسالة نصية أو مباشرة.
- مجاملته في منشور مجهول أو تعليق أو رسالة مباشرة.
- إخباره بأنّك مستعد للإصغاء إذا رغب في التحدّث بعد المدرسة.
- خلال محادثة هادئة شخصيًا أو على الهاتف، يمكنك إخباره بأنّك تعتقد بأنّ السلوك المسيء كان خاطئًا، واسأله إذا كان يرغب بالحديث عما جرى معه.

بغض النظر عن الطريقة التي تختارها للمساعدة، تتوفر لك خيارات علنيّة وأخرى غير علنيّة بهدف **للإبلاغ عن التنمُّر أو الإساءة:** مثل الإبلاغ عبر موقع الويب، أو واجهة التطبيق، أو الإبلاغ عن الحدث لشخص بالغ تثق به.

في كثير من الأحيان عندما ترى شخصًا يتعرض للمضايقة أو الأذى، تريد مساعدته لكنك لا تعرف دائمًا ما عليك فعله، ستعرف خلال الأنشطة أنّك تستطيع مساعدة الآخرين بالطريقة المناسبة لك:

النشاط 1	**مساعدة الآخرين**
الفئة العمرية	11-16 عامًا
الهدف	تعزيز معارف وتوجهات الطلاب/ات حول مساعدة الاخرين عند التعرض لأذى على الإنترنت.
الطريقة	مناقشة السناريوهات، لعب أدوار
الأدوات اللازمة	السناريوهات
التفاصيل	يتوزع الطلاب في مجموعات تقرأ المجموعات المواقف المؤدية وتناقشها معًا يقوم الطلبة باقتراح طرق للتصرف في هذه المواقف، وتسجيلها على اللوح... ثم مناقشة. **الموقف الأول:** ينشر أحد الطلبة مقطع فيديو له وهو يغني أغنية لفنان بوب مشهور، ثم يبدأ طلاب آخرون بنشر تعليقات فظّة أسفل الفيديو، ما الذي يمكنك فعله لدعم الطالب الذي نشر الفيديو؟ استخدم بعض الأفكار التي ناقشناها سابقًا أو اتفِق مع مجموعتك على ردّ جديد. **الموقف الثاني** :اكتشفت بأنّ طالبًا في مدرستك أنشأ حساب تواصل اجتماعي مزيفًا مستخدمًا اسم طالبٍ آخر، ونشر صورًا ومشاركات مضحكة تسخر من طلاب آخرين ومن المعلمين والمدرسة. ماذا تفعل لدعم الطالب الذي تم انتحال هويته بهذه الطريقة؟ فكّر في بعض الحلول التي تمت مناقشتها سابقًا أو اقترح حلاً خاصًا بك. **الموقف الثالث:** اطلب من الطلاب أو الطالبات تأليف موقف وتمثيله

ملاحظات	ملاحظة: لا توجد طريقة واحدة صحيحة لدعم الشخص المستهدف لأن كل شخص– سواء كان مستهدفًا أو متفرجًا– وقد يختلف عن الآخر كما يختلف كل موقف عن الآخر... نحن نحاول فقط تجربة أدوار مختلفة

العنف والابتزاز الإلكتروني

العنف الإلكتروني: هو استخدام أنظمة الكمبيوتر لإحداث أو تسهيل التهديد بالعنف ضد الأفراد، والذي ينتج عنه أو يحتمل أن ينتج عنه أذىً أو ضررًا أو معاناة جسدية أو جنسية أو نفسية أو اقتصادية، وقد يشمل استغلال ظروف الفرد أو خصائصه أو نقاط ضعفه.

أشكال العنف الإلكتروني:

تتنوع أشكال العنف الإلكتروني التي يتم ارتكابها ضد الأفراد، بحيث يمكن تصنيفها بتصنيفات كبيرة، مثل: الجرائم الإلكترونية الجنسية، أو النفسية، أو الاقتصادية، إلخ...

ويمكننا تخصيص الحديث أكثر لتناول أشكال وسلوكيات العنف الإلكتروني كالتالي:

التعرض/ نشر صور أو فيديوهات خادشة للحياء	تشويه السمعة	الابتزاز المادي
اختراق البريد الإلكتروني	التهديد عبر الإنترنت	الابتزاز الجنسي
التوبيخ والتنمّر عبر الإنترنت	التحرّش والمضايقة على الإنترنت	استغلال الصور
انتحال الشخصيات	تلقي/إرسال مكالمات أو عبارات بفحوى جنسي	الانتقام

الابتزاز الإلكتروني:

هو عبارة عن عملية تهديد وتخويف للضحيّة بالتهديد بنشر صور أو فيديوهات أو معلومات حسّاسة أو خاصة عنه، مقابل دفع مبالغ مالية، أو القيام بعمل من نوع معين لصالح المبتزّين، أو بدافع الانتقام.

طرق الابتزاز:

– أغلب عمليات الابتزاز تحدث من خلال بناء علاقة بين المبتزّ والضحيّة، ثم يقوم المبتَزّ بتطوير هذه العلاقة حتى تصل للمحادثات عن طريق مواقع التواصل الاجتماعي، وخلال مرحلة متقدمة من الممكن أن يتحوّل التواصل عن طريق برامج المحادثات المرئية، مثل: تطبيق ماسنجر أو واتساب أو غيرها من تطبيقات المحادثة، ومرةً بعد مرة يقوم الشخص المبتزّ باستدراج ضحيته لمحادثة بمحتوى مسيء وفاضح للضحية، وبعد أن يحصل على مقاطع الفيديو أو الصور المسيئة والفاضحة، أو المعلومات الحساسة، يبدأ بتهديده وابتزازه إما بالمال أو بطلبات غير أخلاقية، وإلّا بإنّ÷ يهدد بتسريب ما لديه بهدف الانتقام.

– طريقة ثانية من طرق الابتزاز تحدث من خلال إرسال روابط أو طلبات صداقة للضحية، وبمجرد الضغط عليها يتم تحميل برامج أو فيروسات تقوم بعمل ثغرات بالنظام الإلكتروني للجهاز المستخدم عند الضحية، وبذلك يستطيع المبتز من خلالها أن يسيطر على جهاز الضحية ويطّلع على المعلومات والصور والفيديوهات وغيرها، وينسخها لجهازه، أو أن يقوم باختراق أحد حساباته على مواقع التواصل الاجتماعي والوصول للمعلومات الخاصة.

من أهم نتائج العنف الإلكتروني (المخاطر والآثار):

- العزلة الاجتماعية، حيث يؤدي إلى انسحاب الضحايا أو الناجيات والناجين من الحياة العامة، بما في ذلك مع العائلة والأصدقاء/الصديقات.
- إمكانية التسبب بدرجة عالية من الأذى النفسي، مثل: الاكتئاب، والقلق، والخوف، وفي بعض الحالات قد تتطوّر إلى ميول انتحارية، علاوةً على الأذى الجسدي كالتسبب في الانتحار.

- الضرر الاقتصادي، بحيث يصبح من الصعب على الضحية العثور على عمل أو حتى منع الضحية من محاولة العثور على عمل؛ بسبب العار والخوف لاحتمالية اكتشاف صاحب العمل للمحتوى، أو اضطرار الضحية لدفع مبالغ مالية لمنع نشر المحتوى.
- قد تجبر أعمال العنف الإلكترونية النساء والفتيات على الانسحاب من الإنترنت، وبالتالي فقدان حقهنّ بالوصول إلى المعلومات، وتشير الأبحاث إلى أنّ 28% من النساء اللواتي عَانَيْن من العنف الإلكتروني القائم على الجنس، قلّلن عمدًا من وجودهنّ على الإنترنت.

في حال تعرضك للتحرّش أو الابتزاز الإلكتروني، عليك فعل التالي:

- لا تتكتم/ي على الابتزاز ولا تتواصل/ي مع المبتزّ تحت أيّ ضغوط.
- توجه/ي لأسرتك كمصدر دعم موثوق لمساعدتك في التعامل مع القضية.
- لا يجب عليك الامتثال إلى طلبات المبتزّ و تأكد/ي أنها لن تتوقف إذا قمت بالخضوع لها.
- عليك بالتواصل مع الجهات الأمنية المختصة في أسرع وقت ممكن، مثل التوجّه لوحدة مكافحة الجرائم الإلكترونية في الشرطة الفلسطينية لتقديم شكوى رسمية، بمساعدة الأهل أو المدرسة.

النشاط 1	**الابتزاز الإلكتروني**
الفئة العمرية	**11 –16 عامًا**
الهدف	تعزيز معارف وتوجهات الطلاب/ات حول الابتزاز الإلكتروني ومخاطره
الطريقة	دراسة حالة ونقاش فعال
الأدوات اللازمة	فيديو
التفاصيل	يتم عرض قصة فتاة أو شاب تعرض للابتزاز الإلكتروني، ويتم توضيح خطوات الموضوع وحلّه، والآثار المترتبة عليه... من ثم يتم فتح نقاش فعّال حول الحالة وتوسيع هذا النقاش.

	يعطي المدرب المجال للطالبات والطلاب أن يؤلّفوا ويمثلّوا قصةً قصيرةً عن محاولة ابتزاز، وكيف تعامل/ت الضحية مع الموضوع. ويوجّه– خلال هذا الوقت– المدرب الطالبات والطلاب نحو الحوار والمناقشة
ملاحظات	يتم عرض قصة الفتاة للطالبات وقصة الشاب للطلاب

النشاط 2	**كيف أعرف؟**
الفئة العمرية	**11–16 عامًا**
الهدف	تعزيز مهارات الطلاب في فهم مواقف التحرّش الجنسي
الطريقة	عمل مجموعات
الأدوات اللازمة	صنوق السلوك فيه مجموعة من السلوكيات (لفئات عمرية مختلفة)
التفاصيل	يتم تقسيم الطلاب/ات إلى مجموعات، بحيث تأخذ كلُّ مجموعة عددًا من السلوكيات، ويتم نقاش هذه السلوكيات إذا كانت تُعدّ تحرشًا جنسيًا. ثمّ يتم شرح السلوكيات التي استقرت عليها المجموعة والتي اتفقوا على كونها تحرشًا... وفتح نقاش فعّال حول الموضوع.
ملاحظات	

النشاط 3	**ما العمل؟**
الفئة العمرية	11 –16 عامًا
الهدف	تعزيز معرفة الطلاب/ات بالحلول الممكن اتخاذها عند الوقوع في مشكلة.
الطريقة	استضافة ممثل/ة من وحدة الجرائم الإلكترونية

الأدوات اللازمة	
التفاصيل	يقوم الضيف من وحدة الجرائم الإلكترونية بنقاش الحلول المقترحة مع الطلاب/ات ومشاركتهم بقصص واقعية ونصائح للوقاية والتعريف بوحدة الجرائم الإلكترونية ودورها.
ملاحظات	

–

القسم الثاني: الفئة العمرية 6-10 أعوام

مقدمة

يسعى هذا الجزء من الدليل للنهوض بتوعية الطلاب والطالبات من جيل 6 أعوام حتى جيل 10 أعوام عن موضوع الأمان الإلكتروني، وحمايتهم من التحرّش والابتزاز على الشبكة، أو الانكشاف على مضامين لا تلائم جيلهم.

وكما هو معلوم فإنّ التطورات التكنولوجية دائمة التغيير، لذا فقد اعتمد هذا الدليل على فعاليات عامة تتطرق للتوجه والتفكير الحذِر الذي نودّ للطالب/ة أن يطوره. وعندما يتطور هذا الفهم العام، تصبح المنصات المختلفة الحالية والمستقبلية أقلّ أهمية؛ لأنّ الطفل طوّرَ التفكير النقدي والحذِر اتجاه المنطق الذي سيحميه.

كلُّ الفعاليات المذكورة أدناه تمت تجربتها، وتم تطوير بعضها على يد مختصّين في مجال التوعية الرقمية. وإنه- قصداً- لم يتمّ حصر الفعاليات لأعمار محددة لإمكانية تمرير هذا الفعاليات للأجيال المذكورة، مع الأخذ بعين الاعتبار ملاءمة الفعالية للجيل.

لقد تمّت كتابة تسلسل الأنشطة كما هي مذكورة هنا لتكون عامّة في البداية، ومن ثم تختص بمواضيع معينة. لكن أي تسلسل آخر يراه المدرب/الاستاذ مناسباً يمكن تبنّيه.

لا تتحدث مع الغرباء:

ينصح الأهلُ دائمًا الأطفال بعدم التحدّث مع الغرباء في الشارع، لكنْ ماذا عن الغرباء على الإنترنت!!

يتواصل الأطفال مع الغرباء كلَّ يومٍ سواءَ كانوا يلعبون ألعابًا عبر الإنترنت مع الأصدقاء، أو ينضمون إلى المحادثات على وسائل التواصل الاجتماعي، والتي تحتوي أيضًا على أشخاص سيئين يختبئون وراء الصور الرمزية لخداع الأطفال بهدف إعطاء تفاصيل شخصية.

يحتاج الأطفال إلى معرفة أنّه من المحتمل ألّا يكون الأشخاص كما يقولون. حتى لو كانت صورتهم أو أصواتهم أو تصرفاتهم كشخص في مثل عمرهم، فقد ينخدع. ساعد الأطفال بإعطائهم بعض القواعد/ مثل: كن حذرًا دائمًا! ولا تُعطِ أيّ معلومات شخصية، حتى للأصدقاء "المعروفين". وقد يشمل ذلك معلومات حول العمر والموقع إلى معلومات تسجيل الدخول عبر الإنترنت، أو سؤال ما إذا كان والداك في المنزل.

أخبر الاطفال أن يتحدثوا مع والديْهم قبل مشاركة معلومات مثل أسمائهم أو عنوانهم أو التحدث مع شخصٍ يقابلونه عبر الإنترنت.

هنالك قاعدة بسيطة للشباب عند الدردشة واللعب مع الآخرين الذين يعرفونهم عبر الإنترنت فقط؛ وهي الالتزام بالدردشة حول اللعبة نفسها، فإذا تغيرت المحادثة وأصبحت أكثر شخصية و/ أو طلب لاعب/ لاعبين آخرين أشياء مثل المعلومات الشخصية للالتقاء في العالم غير المتصل بالإنترنت أو للحصول على صور ومقاطع فيديو، فمن المهم أن يعرض الطفل هذه الرسائل على شخصٍ بالغٍ موثوق به.

تأكد من أنّ الطلاب يعرفون هذه القاعدة وأنهم يعلمون بأنك موجود لمساعدتهم ودعمهم في أيّ شيء يحدث عبر الإنترنت.

قد يكون الالتقاء بشخص ما تعرفه فقط عبر الإنترنت حتى مع صديق أحد الأصدقاء، أمرًا خطيرًا؛ لأنّ هذا الشخص لا يزال غريبًا.

وإذا طلب منك شخصٌ ما تعرفه عبر الإنترنت لقاءك أو الحصول على معلومات شخصية، أو الحصول على صور ومقاطع فيديو لك، فأخبر شخصًا بالغًا على الفور!

النشاط	**الغرباء عبر الإنترنت**
الهدف	تعزيز توجهات الطلاب/ات حول التعامل مع الغرباء على الإنترنت
الطريقة	قصة مصوّرة (هدية العيد)
الأدوات اللازمة	بروجكتر، جهاز حاسوب
التفاصيل	يعرض المدرب/ة القصة المصورة على البروجكتر، وقبل الوصول لنهاية القصة، يتم إيقاف العرض على العبارة رقم (9) يسأل المدرب/ة برأيكم/ن ما الذي يجدر فعله الآن؟ يختار مجموعة من الطلاب لتمثيل النهايات التي قاموا باختيارها ثم يعرض المدرب/ة نهاية القصة... ثم المناقشة
نص القصة	1- في تلك الليلة كان وليد متحمس جدا للنوم، فغداً عيد ميلاده. 2- ها هو اليوم المنتظر، يوم عيد ميلاد وليد، حقًا كانت حفلة رائعة. 3- في نهاية الحفلة قام وليد بفتح الهدايا. وليد: اووووه..! هذا التابلت الذي طالما حلمتُ به، وقَبّل والديه وقال لهما: "شكرًا، شكرًا" 4- والدة وليد قالت له: اذهب للنوم الآن، وغداً سأساعدك للتعلم عليه، ومسموح لك أن تلعب على التابلت ساعة في الصباح، وساعة في المساء فقط. 5- في اليوم التالي عاد وليد للتابلت، قام بتنزيل جميع الألعاب المفضلة لديه وبدء باللعب.

6- كان ينتقل من مرحلة إلى مرحلة في لعبته المفضلة، ويحاول أن يجمع أكبر عدد من الدرجات (scores)

7- فجأة، اهتز التابلت، وظهرت له رسالة:

"مرحبًا، أنا سعيد"

"ما أسمك أنت؟"

فإذا به لاعب آخر يحاول التحدث مع وليد

8- تحمّس وليد للتحدث معه، وقال في فقسه "أصبح لدي أصدقاء على الإنترنت" ثم أجاب: "إسمي وليد".

بعد ذلك أكمل اللاعب.

9- "سأعلمك طريقة لتحصل على الكثير من الدرجات، فنحن شركاء في نفس اللعبة"، وأكمل "قل لي أين تسكن، ومع من".

أراد وليد أن يردّ عليه، وأن يكون لطيفًا معه، لكنّه أيضًا شعر بالقلق قليلًا.

لماذا يسأل عن مكان منزلي؟ فكّر وليد... هل أردّ على هذا اللاعب ونكون أصدقاء، أم أخبر أمي وأبي بدلًا من ذلك؟

10- ذهب وليد إلى والديه مناديًا: "ماما، بابا... هنالك شخص يحاول التحدث معي في اللعبة/ ماذا يجب أن أفعل؟"

11- قال والد وليد: هذا اللاعب طلب معلوماتك الشخصية، لذا عليك أن تحافظ على معلوماتك الشخصية آمنة، ولا تشاركها مع أحد على الإنترنت.

سأل وليد: ما هي معلوماتي الشخصية؟

رد والد وليد: اسمك الكامل، تاريخ ميلادك، مكان منزلك، رقم الهاتف، كلمات السر الخاصّة بك، وغيرها..."

ردّ وليد: " لكنّني أخبرته بأن اسمي وليد".

ردّ والد وليد: "المهم أن لا تُعطِه معلوماتٍ أكثر من ذلك".

12- وأضاف والد وليد: إذا كنتُ لا تعرف الشخص، أو غير متأكد منه وجعلك تشعر بالقلق، أخبرنا فورًا.... ليس جميع الأشخاص الموجودين على الانترنت يتمتعون بالصدق، ولأنّك لا تعرف هذا الشخص في الواقع فإنّه يبقى غريبًا.

دعني أساعدك في منع هذا الشخص من التحدّث معك مرةً أخرى...

13- إذا حدث أي شيء على الإنترنت وجعلك تشعر بالخوف أو القلق أو التوتر اطلب من أحد والديْك المساعدة فورًا.

14- وليد طلب المساعدة من والديه، وأنتَ أو أنتِ مِن مَن تطلب وتطلبين المساعدة؟

ملاحظات	

النشاط	**من** أنت؟
الهدف	تعزيز توجّهات الطلاب/ات فيما يتعلق بعدم تصديق كل شيء تعزيز توجهات الطلاب/ات حول التعامل مع الأشخاص على وسائل التواصل
الطريقة	لعبة "من أنت؟" نقاش فعال
الأدوات اللازمة	الصور
التفاصيل	يُظهر الأستاذُ مجموعةً من الصّور الكبيرة أمام الطلاب لحسابات إلكترونية لمجموعة من الأشخاص المتنوعين، ويسأل الطلاب/ات عن رأيهم في الأشخاص والمعلومات الموجودة عنهم. ومن ثم يخبرهم بأنّه الآن سيقلب أوراق الحقيقة، ليظهر بأنّ العديد من الحسابات من الممكن أن تكون وهمية ولأناس أشرار يريدون أذية الأطفال.
ملاحظات	ليس من الضروري أنّ كلّ الصور فيها اختلافات بين الواقع والخيال؛ لأنّ الهدف الحقيقي تعزيز انتباه الاطفال وليس تخويفهم وإفقادهم الثقة تمامًا. قد تكون بعض الحسابات لأطفال يظهرون أنهم بالغون، الهدف كما ذكر سلفًا تعزيز توجهات الطلاب بأنّ مواقع التواصل الاجتماعي لا تعكس الحقيقة دومًا.

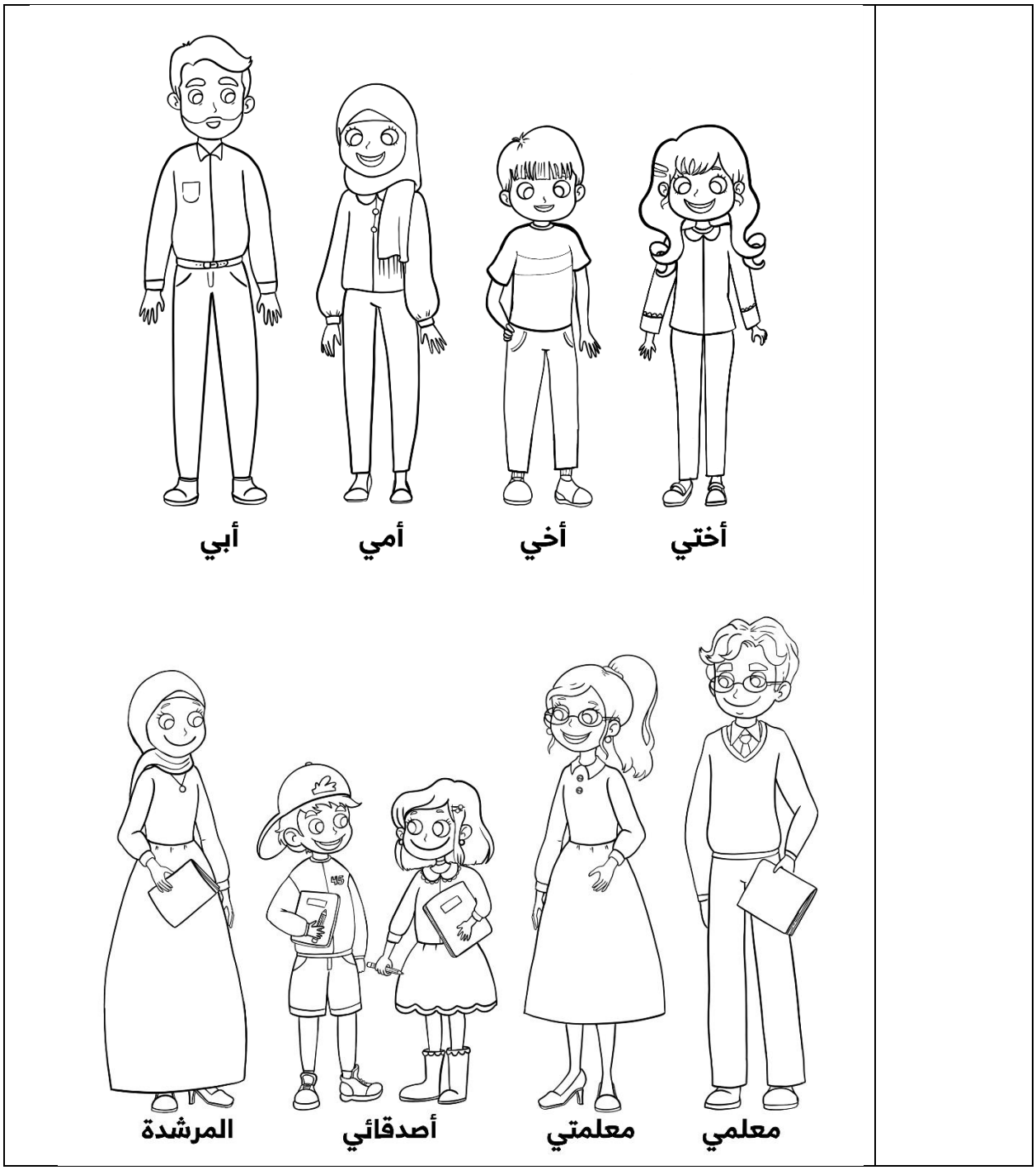
طلب المساعدة

أخبر شخصًا بالغًا موثوقًا به إذا كان هناك شيء أو شخص ما يجعلك تشعر بالضيق أو القلق أو الارتباك، وهذا قد يكون إذا تعرضت أنت أو أي شخص تعرفه للإساءة أو المضايقة عبر الإنترنت، هناك الكثير من الأشخاص القادرين على مساعدتك مثل المعلمين أو والديْك.

النشاط	**ما الذي يجدر فعله**
الهدف	تعزيز معارف الطلاب/ات حول المواقف التي تستدعي طلب المساعدة. تعزيز توجهات الطلاب للتحدث وللإبلاغ في حال تعرضهم/هنّ للإساءة عبر الإنترنت
الطريقة	نقاش ومواقف
الأدوات اللازمة	

التفاصيل	ناقش مع الطلاب: ماذا عليّ أن أفعل إذا كان هناك شخص لا أعرفه إلّا عبر الإنترنت يجعلني أشعر بعدم الارتياح؟ إذا كان هنالك شخص ما تعرفه عبر الإنترنت يطلب منك مقابلتك، أو الحصول على صور أو مقاطع فيديو لك، أو معلوماتك الشخصية. النصيحة هي نفسها لأيّ شيء يجعلك مستاءً أو قلقًا أو مرتبكًا عبر الإنترنت، تحدّث إلى شخص بالغ تثق به. يقوم/تقوم المدرب/ة بعرض مجموعة من المواقف واجهت أطفالًا على الإنترنت. بعد كل موقف يسأل المدرب/ة ما الذي يجب فعله الآن؟

النشاط	**لوّن عالمك**
الهدف	تعزيز معارف الطلاب/ات حول الجهات التي يمكن أن تقدم المساعدة
الطريقة	لعبة لوّن عالمك
الأدوات اللازمة	أوراق رسم عليها الشخصيات الموجودة في عالم الطفل: "الأب، الأم، الأخت، الأخ، الأصدقاء، المرشد، المعلم".
التفاصيل	ورقة يُرسم عليها الشخصيات التي يمكن للطفل أن يتوجّه إليها في حال الحاجة لمساعدة، ويمكن الطلب من الأطفال أن يلوّنوا أهمّ 3 شخصيات يمكن أن يتوجهوا إليها. يمكن أن تمثل الشخصيات كلًا من الأب، الام، الأخت، الأخ، الأصدقاء، المرشد، المعلم.
ملاحظة	بالنسبة للأصدقاء فالمسألة شائكة، لأنّ الأصدقاء في الغالب بنفس الجيل، وليس من المؤكد أن يقدموا نصيحة صحيحة. لكن من الممكن أن يثق بهم الطفل أكثر لأنهم يتفهمون الموقف أكثر. الرسومات :



أهمية الإيجابية واللطافة عبر الانترنت:

من المهم عدم جعل الإنترنت بالكامل يبدو مكانًا مخيفًا، لتجنب ذلك بأي ثمن ساعد في تمهيد الطريق للسلوك المسؤول عبر الإنترنت من خلال التحدث عن الطرق التي يمكن أن يساعد بها الإنترنت في العمل المدرسي ومتابعة اهتمامات أخرى.

أخبر الطلبة عن أهمية أن يكونوا لطفاء دائمًا ومحترمين مع الآخرين عبر الإنترنت.

النشاط	كيف نشعر
الهدف	تعزيز توجهات ومهارات الطلاب/ات في التعامل بلطف على الانترنت.
الطريقة	نقاش فعال
الأدوات اللازمة	وجوه تحمل تعبيرات مختلفة (ايموجي) التعليقات
التفاصيل	يقوم المدرب بوضع تعليقات على الإنترنت بعضها سلبي وبعضها إيجابي على اللّوح ويطلب من كلّ طالب أن يعتبر أنها موجهة له ثم يطرح أسئلة "كيف يشعر؟" يقوم الطلبة بإلصاق الوجه الذي يعبر عن شعورهم/نّ ثم يقوم بنقاش مفاده أنّ الأشخاص الآخرين على الإنترنت يتأثرون بماذا نكتب عنهم أو نعلّق عليهم، كما أثّرت علينا هذه العبارات. أمثلة على التعليقات: سيرتدي الجميع اللون الأحمر غدًا، ولكن لا تخبروا ليلى ما هذه الصورة، أنت غبي أنت مضحك وأحمق صوتك جميل جدًا، لم أكن أعرف هذا لا أقصد الإهانة، لكنّك لا تُجيد اللعب أنت رائع وموهوب يسعدني أنّك صديقي أنا غاصب جدًا منك، نتقابل في المدرسة غدًا لا يهمّنا رأيك، لماذا تشاركه هههههه
الملاحظات	

وقت الشاشة والتوازن الصحي

ما هو وقت الشاشة؟

وقت الشاشة هو مقدار الوقت الذي تقضيه أمام الشاشة على أي جهاز، وتوفر الأجهزة الرقمية العديد من الفرص الرائعة لجميع أفراد الأسرة، بما في ذلك أنشطة التعلم والإبداع، فضلًا عن الترفيه والاستمتاع. ومع ذلك، نسمع من الآباء ومقدمي الرعاية أن إدارة وقت الشاشة يمكن أن تكون مصدرًا للصراع مع أطفالهم عندما يتعلق الأمر بالأطفال والتكنولوجيا، ولطالما طرح الآباء ومقدمو الرعاية نفس السؤال:

ما هي مدة الشاشة المناسبة للطفل؟

أصدرت الكليّة الملكية لطب الأطفال وصحة الطفل (RCPCH) إرشادات بشأن وقت الشاشة لمن هم دون سن 18 عامًا. بالاعتماد على الأبحاث والدراسات حول تأثيرات وقت الشاشة، وخلصوا إلى أنّه لا يوجد "موصى به" أو "مقدار محدد" من الوقت يجب أن يقتصر على الأطفال على الأجهزة. وبدلًا من ذلك، يجب أن يكون التركيز على ضمان ألّا يحلّ الوقت الذي تقضيه على الأجهزة محل النوم أو ممارسة الرياضة أو وقت الأسرة. وينصحون بضرورة تجنب الأجهزة في الساعة التي تسبق النوم لتعزيز النوم الصحي، وقد قدموا قائمة المراجعة التالية لمساعدة الآباء ومقدمي الرعاية على اتخاذ قرارات بشأن استخدام عائلاتهم للشاشة:

هل وقت شاشة تحت السيطرة؟

هل يتعارض استخدام الشاشة مع ما يجب القيام به؟

هل يتعارض استخدام الشاشة مع النوم؟

هل أنت قادر على التحكم في تناول الوجبات الخفيفة أثناء وقت الشاشة؟

الحدّ من وقت الشاشة للأطفال:

أولًا، ضع حدودًا للوقت على الإنترنت.

عندما لا يكون وقتهم على الإنترنت كبيرًا، تكون هناك فرصة أقل للانجراف إلى أجزاء غير مرغوب فيها من الإنترنت.

كم من الوقت يجب أن يقضيه الطفل على الإنترنت؟

هذا سؤال صعب حقًا! لا يعتقد خبراء التكنولوجيا أن هناك قدرًا مثاليًا من الوقت لقضائه على الإنترنت، ويقولون إنّه من المهم التركيز على استغلال الوقت على الإنترنت جيدًا. لكنْ، لتسهيل الموضوع للأطفال والطلاب، من الممكن أن يتمّ إعطاؤهم وقتًا محددًا يُتفقُ عليه مع الأهل أو المرشد.

النشاط	الاتفاقية
الهدف	تعزيز توجهات الطلاب/ات حول الوقت المعقول للجلوس على الإنترنت.

الطريقة	نقاش، عمل اتفاقية
الأدوات اللازمة	
التفاصيل	يبدأ المدرب بإدارة نقاش من خلال الأسئلة التالية: فكّر فقط في كلّ الأشياء المختلفة التي تستمتع بعملها عبر الإنترت. فكر الآن! بأيٍّ منها تستمتع أكثر؟ ما الذي تقضي معظم وقتك في فعله؟ وما هي الأفضل؟ عمل اتفاقية مكتوبة بين المدرب والطلاب لتحديد وقت الشاشة، فمن المرجح أن يتبعهم الأطفال إذا اعتقدوا أنهم لعبوا دورًا في وضعها. ضع حدودًا معقولة للتأكد من أنّ الشاشات الرقمية لا تحلّ محلّ تفاعلات الحياة الواقعية والنشاط البدني.
الملاحظات	من الممكن أن يتمّ تعليق الاتفاقية على حائط الصف.

اللعب على الإنترنت

يوجّه المرشد الطلبة للنصائح التالية:

يمكن أن يكون اللعب مع أصدقائك عبر الإنترنت ممتعًا للغاية، لكنْ في بعض الأحيان يمكنهم فعل وقول أشياء ليست لطيفة جدًا. وفيما يلي أهم النصائح لممارسة الألعاب عبر الإنترنت مع لاعبين آخرين:

إذا كنت تلعب مع أشخاص لا تعرفهم، فتذكّر عدم مشاركة أيّ معلومات شخصية أو تفاصيل عنك، على سبيل المثال: ما اسم مدرستك؟ أو المكان الذي تعيش فيه، أو كلمات المرور الخاصة بك.

إذا قال أو فعل أيّ شخص أيّ شيء يثير قلقك أو يزعجك، فتحدّث إلى شخص بالغ تثق به للحصول على المساعدة والدعم.

النشاط	**اللعب على الإنترنت**
الهدف	تعزيز توجهات الطلاب/ات حول التصرفات السليمة عند اللعب مع الآخرين
الطريقة	عمل مجموعات
الأدوات اللازمة	

التفاصيل	يبدأ/تبدأ المدرب/ة الحوار بسؤال: ما الألعاب التي تفضلونها على الإنترنت؟ من أشهر الألعاب Maincraft– Roblex– Pubg مع من تلعبون؟ يقسم المدربُ اللّوح لقسميْن: تصرف سليم، وتصرف خاطئ. ويطلب من الطلبة كتابة ما هي التصرفات السليمة، وما التصرفات الخاطئة فيما يتعلق باللعب على الإنترنت.
ملاحظات	حتى يتسنى للمدرّب أن يعطي أمثلة قريبة من عالم ألعاب الأطفال من المفضل فحص ما هي الألعاب المشهورة في تلك الفترة. وأيّ منها تكون مع لاعبين آخرين على الشبكة.

الإعلانات:

الإعلانات هي طرق للشركات لتظُهر لك مواقع الويب والتطبيقات والأشياء الأخرى التي يمكنك شراؤها. وعادةً ما يتم تصميم الإعلانات عبر الإنترنت لإقناعنا على النقر عليها، يمكن أن تظهر في شكل نوافذ منبثقة أو أشرطة جانبية أو ملء الشاشة في أحد التطبيقات.

من الأفضل دائمًا تجنب النقر على الإعلانات، لأنك لا تعرف إلى أين ستأخذك، ولكن قد يكون من الصعب أحيانًا اكتشافها.

كيف تعرف الإعلانات:

أيّ شيء يبدو مختلفًا عن محتوى الصفحة أو اللعبة في حال استخدام الجوال.

أيّ شيء لم تكن تتوقع ظهوره.

أيّ شيء يريدك أن تضغط عليه، مثل: أداة دوارة أو مهمة تفاعلية أو ارتباط إلى موقع آخر.

إذا رأيت إعلانًا، فحاول تجنّب النقر عليه، وليكن معلومًا بالنسبة لبعض إعلانات الفيديو، فإنّك قد تحتاج إلى السماح بتشغيلها حتى النهاية قبل أن تتمكن من العودة إلى لعبتك. وبالنسبة لبعض النوافذ المنبثقة، قد يكون هناك x صغير في الزاوية يمكنك استخدامه لإغلاق الإعلان.

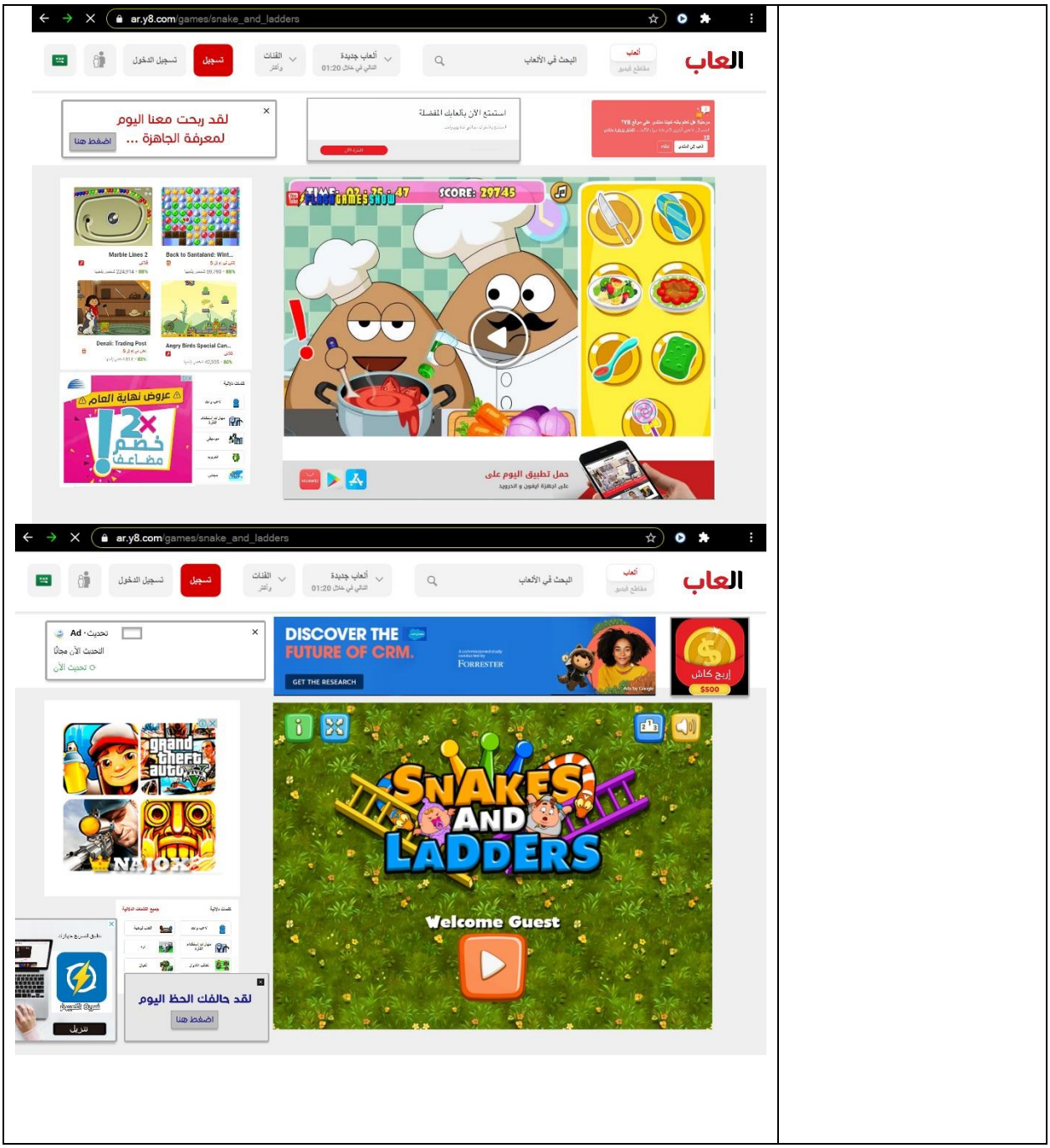
تذكر!

- إذا رأيت أيّ شيء في إعلان مزعج أو غير مناسب، فأخبر شخصًا بالغًا على الفور.

- إذا نقرت بالخطأ على إعلان، فلا داعي للقلق. لا يزال بإمكانك التحدث إلى شخص بالغ والحصول على المساعدة.
- إذا كانت اللعبة تحتوي على الكثير من الإعلانات وتزعجك، فقد حان الوقت لتجربة لعبة جديدة!

أو يمكنك استخدام الوقت الذي يظهر فيه الإعلان لأخذ استراحة... تناول مشروبًا أو دردش مع عائلتك، ثم تعود إليها لاحقًا.

النشاط	**أين الإعلان ؟**
الهدف	تعزيز معارف الطلاب /ات حول الاعلانات وتمييزها في الصفحة
الطريقة	مثال
الأدوات اللازمة	مثال الصفحة الإلكترونية
التفاصيل	يعرض المدرب/ة أمثلة للإعلانات التي من يمكن أن تظهر على الشاشة أثناء اللعب وكيف يتم إغلاقها. يقوم المدرب/ة بتوزيع ورقة تمثل صفحة للعبة إلكترونية مع وجود إعلانات منبثقة، وعلى الطالب تمييز الإعلانات وقصّها. ثم يتم نقاش أهم الأمور التي جعلتهم يميّزون الإعلانات وكذلك أهمية إغلاقها فورًا. فكر مليًا قبل النقر فوق شيء ما عبر الإنترنت أو فتحه، مثل: الروابط والإعلانات وطلبات الصداقة والصور. حيث لا تعرف أبدًا إلى أين قد تؤدي، أو ربما قد تحتوي على فيروسات. لا تقبل شيئًا إذا كنت غير متأكد من هوية الشخص المرسل أو ما الذي أرسله إليك.
الملاحظات	من الممكن تعريف الطلاب على إضافات المتصفح التي تمنع الإعلانات من الظهور أو مشاركة مصادر عن الموضوع. https://ar.wizcase.com/blog/أفضل-مانعي-الإعلانات-في-عام/ امثلة :



YouTube يوتيوب

هناك محتوى جيد تعليمي وممتع على YouTube لكن حتى هذا يجب أن يُنظر إليه باعتدال.

عندما يتعرض الأطفال لمجموعة واسعة من المحتوى على YouTube فإنّ ذلك يثير القلق؛ لأنّ المحتوى قد لا يكون مناسبًا للفئة العمرية، مما قد يدفعهم إلى رؤية شيء ليسوا ناضجين بما يكفي للتعامل معه. هناك الكثير من مقاطع الفيديو المخيفة أو كما هو الحال مع الأشكال الأخرى من وسائل التواصل الاجتماعي، لا يخلو موقع YouTube من نصيبه من الإعلانات الممولة، ولكن يبدو أنّ هناك مشكلة جديدة تظهر وهي الأساليب الإعلانية المخادعة التي تستهدف الأطفال الصغار، وفي بعض الأحيان لا يمكن تخطّيها.

النشاط	اليوتيوب
الهدف	تعزيز توجهات ومهارات الطلاب/ات في التعامل مع موقع يوتيوب.
الطريقة	نقاش مع أسئلة للأطفال
الأدوات اللازمة	
التفاصيل	من المفضل البداية بسؤال مفاده: من يستخدم اليوتيوب؟ ثم السؤال عن طول الاستخدام، ثم السؤال عن لماذا هذه الفترة؟ وهل لأن الأهل يحددون الوقت؟ أو لأن الطفل يملّ؟ أو لأن عليهم القيام بالواجبات؟ إلخ... بعدها من الممكن أن يوجّه سؤالًا للطلبة عن قنواتهم المفضلة وماذا تعرض.
الملاحظات	على الأستاذ أن يحاول الإشادة بالسلوك الحسن والمحبذ اتباعه، لكنْ عليه كذلك أنْ يحذّر من التوبيخ أو الإشارة لطالب بعينه كمثال سيء. وأمّا الهدف الإضافي للمذكور أعلاه هو التحفيز على تشغيل المحتوى الذي يتناسب مع عمر الأطفال في حال شارك الأطفال قنوات تتناسب مع عمرهم عند فحصهم لقنوات أصدقائهم.

من الممكن مشاركة الأهل بموقع https://www.youtubekids.com وهو جزء من مجموعة يوتيوب مطور ومخصص للأطفال. بحيث يتيح الموقع للأهل السماح بقنوات معينة ومضامين محددة تتناسب مع الأجيال المختلفة (أصغر من ٤ أعوام، ومن 4–8 أعوام، ومن8–12 عامًا). ويمنع الموقع الإعلانات الممولة بشكل قاطع، علمًا أن الموقع لا يزال تحت التجربة، ولم تطلقه جوجل لغاية الآن بشكل رسمي، لكنه بديلٌ ممتاز عن إتاحة كلِّ المضامين على يوتيوب.

للمزيد عن المشروع https://www.youtube.com/intl/ar/kids/

بدائل ومكمّلات للإنترنت

يمكن أن تكون الألعاب واحدةً من أفضل الطرق للاستمتاع عبر الإنترنت، لكنّها بالنسبة لبعض الأشخاص يمكن أن تصبح

هوسًا بعض الشيء.

لكنْ، هل أنت حقًا مدمنٌ على لعبتك المفضلة؟ أو على مواقع التواصل الاجتماعي؟ أو حتى على الإنترنت بشكل عام؟

على الاغلب لا!

لا نستخدم كلمة "مدمن" غالبًا لأنها تجعل الأمر يبدو وكأنه ليس لديك سيطرة. لكنْ، تذكّر أنّه يوجد دائمًا شيء ما يمكنك فعله إذا كانت اللعبة تدور في ذهنك كثيرًا، مثل:

- التحدث الى شخص ما.
- خذ فترات راحة منتظمة: سيعطي هذا عقلك استراحة من اللعبة والإنترنت، وسيمنحك فرصةً للتفكير أو القيام بشيء مختلف!
- حاول العثور على بعض الأشياء الأخرى التي تستمتع بها، مثل نشاط غير متصل بالإنترنت كالرّياضة، واستخدمه لتحقيق التوازن بين الوقت الذي تقضيه في ممارسة الألعاب.

تذكر!!

لقد صُممت الألعاب لتكون ممتعة ومثيرة، ولكي تجعلنا نعود إليها في كلّ مرة، لكنّك أنت وعائلتك مسؤولون عن عدد المرّات والوقت الذي تلعب فيه.

النشاط	ارسم ماذا تحب
الهدف	تعزيز توجهات الطلاب حول التفكير في أنشطة بديلة عن الإنترنت
الطريقة	الرسم
الأدوات اللازمة	أوراق، ألوان
التفاصيل	يحثّ/تحثّ المدرب/ة الطلاب على التفكير فيما يفضلون القيام به في حال عدم وجود إنترنت. ثم يطلب من كل طالب رسم أمورٍ تدلّ على هذا، فمثلًا: إذا كان يُحبُّ لعب كرة القدم، فإنّه يرسم كرة، وإذا كان يُحبُّ الرسم يقوم برسم علبة ألوان ثم يقوم بإلصاق جميع الرسومات على اللّوح. بعد ذلك يتم نقاشها كأفكار لقضاء الوقت من دون إنترنت.
الملاحظات	

المصادر :

Google_Be Internet Awesome

https://myshadow.org/ar

https://securityinabox.org/ar

https://ssd.eff.org/ar

مركز حملة

https://digital-protection.tech

الكلية الملكية لطب الأطفال وصحة الطفل(RCPCH)

Childnet

نبذة عن تام :

جمعية تنمية واعلام المرأة (تام) هي منظمة فلسطينية اهلية غير حكومية تأسست في عام 2004 ومقرها الرئيس في بيت لحم. تسعى تام إلى تحقيق مجتمع حر وديمقراطي، يسوده العدل والمساواة واحترام حقوق الإنسان، حيث تتمتع المرأة بحقوقها وبالمساواة دون تمييز. تعمل تام على تغيير الثقافة السائدة، والصورة النمطية للمرأة من خلال اعلام حر حقوقي ونسوي، ومن خلال تمكين وتدعيم مؤسسات اعلامية واعلاميين/ات على النوع الاجتماعي والحقوق كما نسعى لتمكين النساء والفئات في كافة المجالات لتحقيق أهدافهم/ن وتطلعاتهم/ن.

العنوان: بيت جالا- السهل والصريصير- شارع جايل العرجا – عمارة ابو عبيدة الطابق الاول.
بيت لحم – الضفة الغربية – فلسطين
صندوق بريد: 826 بيت لحم
هاتف: 022760496 ، فاكس، 022753727
ايميل: info@tam-media.org

فيسبوك : تنمية وإعلام المرأة/ تام Women Media and Development/ TAM
https://www.facebook.com/TamWomenMedia
توتير: @WomenTam
https://twitter.com/WomenTam
انستجرام: tam_media
https://www.instagram.com/tam_media/?hl=en
الموقع الالكتروني : tam.ps
يوتيوب : تنمية و إعلام المرأة/ تام Women Media and Development/ TAM
https://www.youtube.com/channel/UC1vhPZ4EEtaB_zzSdoL2Iug
منصة كوني بأمان : besafe.ps
https://www.besafe.ps/