

استخدام الإنترنت

بذكاء

بحذر

بثقة

بلطف

بشجاعة

أبطال
الإنترنت

أبطال الإنترنت

أهلاً بك في منهج "أبطال الإنترنت" الدراسي، الذي تم تطويره بالتعاون بين Google وجمعية Internet Keep Safe Coalition (iKeepSafe.org). ويُسكّل هذا المرجع جزءاً من برنامج "أبطال الإنترنت" المتنوع والمصمّم لتعليم الأطفال المهارات الضرورية لاستخدام الإنترنت بأمان وذكاء.

يزوّد منهج "أبطال الإنترنت" الدراسي المعلمين بالأدوات والأساليب اللازمة لتدريس أساسيات الأمان على الإنترنت والمواطنة الرقمية. كما تُبرز خطط الدروس أهم المعلومات التي يمكن أن يزوّد بها المعلمون طلابهم، لإعدادهم للمواطنة الرقمية السليمة والاستخدام الآمن للإنترنت. ويمكن تعزيز هذه الدروس والمفاهيم من خلال لعبة "عالم الإنترنت" (g.co/abtalinternet)، وهي لعبة على الإنترنت مليئة بالمغامرات وتوفّر تجربة تعلّم تفاعلية وممتعة عن الأمان والمواطنة الرقمية.

تتألف مدونة سلوك "أبطال الإنترنت" من خمس مواضيع أساسية في مجال الأمن الرقمي والمواطنة الرقمية وهي:

- شارك بانتباه (استخدام الإنترنت بذكاء)
- لا تصدّق الخدع (استخدام الإنترنت بحذر)
- احم أسرارك (استخدام الإنترنت بثقة)
- اللطافة من سمات الأبطال (استخدام الإنترنت بلطف)
- اسأل واستفسر (استخدام الإنترنت بشجاعة)

وعلى الرغم من أنّ هذه الدروس مصمّمة لتناسب الطلاب من الصف الثالث وحتى السادس، إلا أنّ معلمي الصفوف الأكبر أو الأصغر سنّاً وجدوا هذا المنهج الدراسي مفيداً لطلابهم، نظراً لما يقدّمه من معلومات قيّمة مثل المصطلحات الأساسية والمناقشات (التي يمكن تعديلها لتلائم سنّ الطلاب) وتجربة اللعبة. ونحن نشجّع المعلمين على الاختبار لتحديد أفضل العناصر المناسبة لطلابهم، سواء كان ذلك عبر تعليم المنهج بأكمله أو التركيز على بعض الدروس الأكثر أهمية ضمن محيطهم التعليمي.

والجدير بالذكر أنّ الجمعية الدولية للتكنولوجيا في التعليم (ISTE) أتمت تدقيقاً مستقلاً لمنهج "أبطال الإنترنت"، واعتمدته كمرجع دراسي يساعد على إعداد الطلاب لاستيفاء معايير ISTE للطلاب للعام 2016. كما منحت الجمعية منهج "أبطال الإنترنت" شهادة التميّز Seal of Alignment Readiness.

يُسكّل كلّ من منهج "أبطال الإنترنت" ولعبة "عالم الإنترنت" اثنين من المراجع العديدة المتاحة للأهل والمعلمين لتعزيز استخدام الإنترنت بوعي وأمان. ويمكنك زيارة موقع g.co/BelInternetAwesome للحصول على المزيد من المراجع من Google، مثل الفيديوهات التعليمية للمعلمين والمواد التعليمية القابلة للتنزيل وأدوات الدمج التقني المفيدة.



جدول المحتويات

| | |
|----|---|
| 4 | دليل المعلمين المرجع الأول: نموذج البريد الإلكتروني/الرسالة التمهيدية للأهل المرجع الثاني: الأسئلة الشائعة |
| 8 | الدرس الأول: شارك بانتباه النشاط 1: الحالات التي يجب عدم المشاركة فيها النشاط 2: لمن هذا الملف الشخصي؟ النشاط 3: كيف يرانا الآخرون؟ النشاط 4: الحفاظ على الخصوصية النشاط 5: "عالم الإنترنت": جبل المشاركة |
| 20 | الدرس الثاني: لا تصدّق الخدع النشاط 1: لا تقع في فخ التصيد الاحتيالي! النشاط 2: من أنت حقاً؟ النشاط 3: حول الروبوتات النشاط 4: "عالم الإنترنت": نهر الحقيقة |
| 38 | الدرس الثالث: احجم أسرارك النشاط 1: كيف تختار كلمة مرور قوية النشاط 2: كيف تحتفظ بها لنفسك النشاط 3: "عالم الإنترنت": قلعة الأمان |
| 46 | الدرس الرابع: اللطافة من سمات الأبطال النشاط 1: من متفرجين إلى مدافعين النشاط 2: خيارات المدافعين النشاط 3: ولكن قل ذلك بلطف! النشاط 4: انتبه لنبرتك النشاط 5: قبول التحدي النشاط 6: "عالم الإنترنت": مملكة اللطافة |
| 62 | الدرس الخامس: اسأل واستفسر النشاط 1: متى يجب طلب المساعدة النشاط 2: الإبلاغ أيضاً على الإنترنت |

دليل المعلمين: المصدر الأول نموذج البريد الإلكتروني/الرسالة التمهيدية للأهل

في ما يلي نموذج لرسالة خطية أو إلكترونية يمكنك تعديلها والتي تهدف إلى إطلاع الأهل على الأدوات التعليمية الجديدة المستخدمة في تعليم أطفالهم كيفية اتخاذ قرارات صائبة بشأن سلوكهم وأمانهم على الإنترنت.

الأهل الأعزاء،



عندما يكون أطفالنا صغارًا، نبذل قصارى جهدنا لمساعدتهم على الاستفادة إلى أقصى حدّ من الإنترنت من جهة، وحمايتهم من مخاطرها وسلبياتها من جهة أخرى. وعند بلوغهم سن المراهقة، يتحوّل دورنا إلى مساعدتهم في تعلّم كيفية اتخاذ قرارات آمنة ومدروسة في العالم الرقمي.

نحن في [اسم المدرسة] نؤمن بالشراكة مع الأهل وإعداد طلاب [الصف] لما يلي:

- التفكير النقدي وتقييم مواقع الويب وعناوين البريد الإلكتروني والمحتويات الأخرى على الإنترنت.
- حماية أنفسهم من التهديدات الموجودة على الإنترنت، بما في ذلك التنمّر ومحاولات الخداع.
- المشاركة بحذر: الانتباه للمحتوى الذي يشاركونه ووقت وكيفية مشاركته، إضافة لمن يشاركونه معه.
- التعامل بلطافة واحترام مع الآخرين على الإنترنت، بما في ذلك احترام خصوصيتهم.
- طلب المساعدة في المواقف الصعبة من الأهل أو شخص بالغ موثوق به.

ستشمل هذه الجهود خلال هذا العام برنامج "أبطال الإنترنت" المتنوّع والمصمّم لتعليم الأطفال المهارات الضرورية لاستخدام الإنترنت بأمان وذكاء، ولعبة "عالم الإنترنت" التي توفّر تجربة تعلّم تفاعلية وممتعة على الإنترنت. يوفّر برنامج "أبطال الإنترنت" الذي طوّره Google بالشراكة مع معلمين وباحثين وخبراء في مجال الأمان على الإنترنت في iKeepSafe.org تجربة تعلّم ممتعة مناسبة لأعمار معيّنة وتتألف من خمسة دروس أساسية:

- شارك بانتباه
- لا تصدّق الخدع
- احم أسرارك
- اللطافة من سمات الأبطال
- اسأل واستفسر

يشجّع استخدام التكنولوجيا الذكي والامن الطلاب على التعلّم ويساعد في تحسين أداء مدرستنا. نحن نؤمن بأن برنامج "أبطال الإنترنت" سيكون بمثابة خطوة مهمة نحو تحقيق هدفنا المتمثّل بضمان مشاركة جميع طلابنا في [اسم المدرسة] في التعلّم والاستكشاف واستخدام الإنترنت بأمان، داخل المدرسة خارجها.

سيسرنا مشاركة المزيد من المعلومات حول هذا البرنامج الجديد، بما في ذلك مقدمة لبعض المراجع التي سيستخدمها الطلاب في الصف، و ندعوكم للاطلاع على المراجع المتوفرة للأهل على الرابط g.co/abtalinternet. وننصح بسؤال الطلاب عن الأنشطة التي يشاركون فيها ومتابعة مناقشة هذا الموضوع في البيت، وقد تستفيدون بأنفسكم من بعض النصائح المتعلقة بالأمان والخصوصية!

مع أطيب التحيات،

[الاسم]

الأسئلة الشائعة

هل من الضروري إكمال الدروس قبل بدء لعبة "عالم الإنترنت"؟
كلا، ولكننا نوصي بإكمال الدروس قبل البدء باللعبة، والتي يمكن الاستفادة منها لتعزيز المفاهيم المكتسبة خلال المنهاج الدراسي. كما أنّ الطلاب قد يستفيدون من فرصة التواصل معك خلال جلسات النقاش والعصف الذهني قبل البدء باللعبة.

هل يحتاج الطلاب إلى حسابات **Google** للدخول إلى منهاج "أبطال الإنترنت"؟
كلا، المنهاج متاح لجميع زوّار الموقع الإلكتروني، ولا حاجة إلى تسجيل الدخول أو استخدام كلمات المرور أو عناوين البريد الإلكتروني.

ما هي الأجهزة المتوافقة مع لعبة "عالم الإنترنت"؟
تعمل لعبة "عالم الإنترنت" على أي جهاز متّصل بالإنترنت ويحوي متصفّح ويب. وبالتالي، فإن جميع أجهزة الكمبيوتر أو الأجهزة اللوحية أو الهواتف الجوّالة تقريبًا ملائمة لمساعدتك في أن تصبح بطلاً من أبطال الإنترنت.

ما هي عناوين **URL** ذات الصلة؟
• للدخول إلى الصفحة الرئيسية في موقع "أبطال الإنترنت"، انتقل إلى g.co/abtalinternet
• للدخول إلى لعبة "عالم الإنترنت"، انتقل إلى g.co/abtalinternet
• للدخول إلى منهاج "أبطال الإنترنت" الدراسي، انتقل إلى g.co/abtalinternet

هل أحتاج إلى تدريب خاص أو امتلاك خلفية معيّنة في مجال التدريس لإكمال المنهاج؟
• أولاً: يمكن لأي معلم مؤهل لتعليم الصفوف الأول حتى الثاني عشر تدريس هذا المنهاج لطلابه. ليس هناك حاجة لأي تدريب إضافي.
• ثانياً: كل معلم متميز. (:

ما هي الصفوف التي يلائمها منهاج "أبطال الإنترنت"؟
تم تصميم البرنامج الكامل، بما في ذلك المنهاج واللعبة والمراجع على الموقع، للمستخدمين من الصف الثالث إلى السادس (من سن 8 إلى 12 عامًا). ولكن يمكن للمعلمين تكييف المنهاج بحيث تكون مواضيعه مفيدة لأي من الصفوف.

كيف يتعلم الأطفال من اللعبة؟
تعزز اللعبة المفاهيم الواردة في المنهاج من خلال السماح للطلاب باستكشاف الممارسات الرقمية السليمة من خلال اللعب وفهم التفاعلات الرقمية (وعواقبها) في بيئة تعليمية آمنة.

هل يمكن استخدام كل من الدروس في **Google Classroom**؟
نعم، بكل تأكيد. يمكنك تخصيص لعبة "عالم الإنترنت" لصفوف أو طبقات معينة، أو إتاحة المرجع لجميع الطلاب في شكل إعلان للصف.

هل هناك مجلد أو موقع ويب مشترك فيه أوراق عمل يمكن الوصول إليها بسهولة وعرضها على لوح المعلومات؟

نعم، وهي متوفرة على شكل بطاقات عرض، حيث تعاوننا خلال التحديث الأخير للمنهاج مع Pear Deck على وضع منهاج "أبطال الإنترنت" بهذا الشكل لتسهيل تقديمه وتوزيعه ومشاركته. ويمكنك الاطلاع عليها على الرابط.

<https://beinternetawesome.withgoogle.com/ar/resources>

هل يجب أن أكون خبيرًا في المواطنة الرقمية لاستخدام هذا البرنامج؟ كلا، على الإطلاق. تم تصميم هذا المنهاج الدراسي بحيث يمكن لأي معلم الوصول إليه وتدريبه في صفه. وإذا كنت ترغب في التعمق أو تعلم المزيد حول مجال الأمان الرقمي والمواطنة الرقمية، يمكنك المشاركة في دورتنا التدريبية على الإنترنت للمعلمين عبر الرابط

edutrainingcenter.withgoogle.com/digital_citizenship/preview

هل يتوافق منهاج "أبطال الإنترنت" مع أي معايير وطنية أو معايير الولاية؟ سؤال ممتاز. نعم، يتوافق منهاج (أبطال الإنترنت) مع معايير الجمعية الدولية في التعليم (ISTE) والرابطة الأمريكية لأمناء المكتبات المدرسية (AASL).

هل يمكن للطلاب حفظ التقدّم الذي حققوه في لعبة "عالم الإنترنت"؟ ليس في الإصدار الحالي، وليس من المرجح أن يتغير ذلك. لا يُنشئ منهاج "أبطال الإنترنت" أو يُخزّن أي معلومات تعريف شخصية على الإطلاق، بما في ذلك ملفات الحفظ. ويعود ذلك إلى رغبتنا في جعل هذه التجربة في متناول الجميع بدون الحاجة إلى حساب أو تسجيل الدخول أو إدخال كلمة مرور.

هذا أمر جيد، ولكن الكثير من طلابي فخورون بإنهاء اللعبة وبما تعلموه. نحن ندرك ذلك، ولهذا السبب أنشأنا نموذج شهادة يمكن تعديله عبر إدخال اسم الطالب وإنشاء شهادة مخصصة قابلة للطباعة للطلاب الذين أكملوا الدورة.

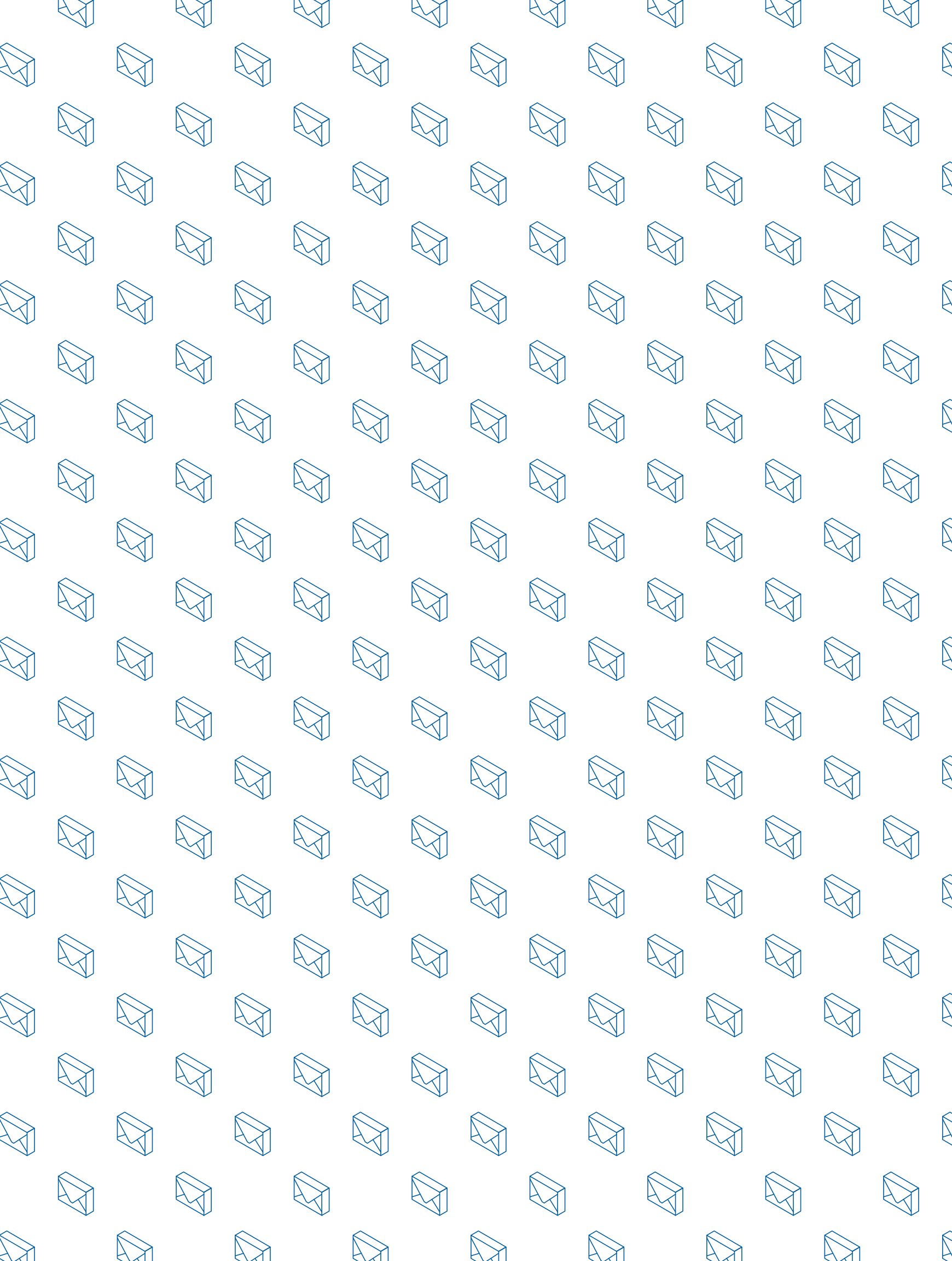
أين يمكنني العثور على مراجع أخرى مخصصة للمعلمين؟ يمكن العثور على جميع مواد منهاج "أبطال الإنترنت" المخصصة للمعلمين في صفحة المراجع على الرابط

<https://beinternetawesome.withgoogle.com/ar/resources>

هل يوجد منتدى على الإنترنت لمستخدمي منهاج "أبطال الإنترنت" لمشاركة الأفكار أو الحصول على المساعدة؟

نعم، لدينا منتدى على Twitter نشارك فيه الأفكار ونتواصل عبره مع المعلمين باستمرار. ويرجى متابعتنا للحصول على المزيد من المعلومات حول منهاج "أبطال الإنترنت" ومواضيع أخرى على الحساب [@GoogleForEducation](https://twitter.com/GoogleForEducation).

ملاحظات



شارك بانتباه

حماية نفسك وسمعتك على الإنترنت

- النشاط 1: الحالات التي يجب عدم المشاركة فيها
- النشاط 2: لمن هذا الملف الشخصي؟
- النشاط 3: كيف يرانا الآخرون؟
- النشاط 4: الحفاظ على الخصوصية
- النشاط 5: "عالم الإنترنت": جبل المشاركة

نظرة عامة على الدرس

يدرك المعلمون والأهل كيف يمكن للأخطاء المرتكبة في العالم الرقمي أن تؤذي المشاعر وتُضرب بالسمعة والخصوصية. ولكن قد يصعب إقناع الأطفال بأن المشاركات التي تبدو سليمة لهم قد تُضربهم في الحاضر أو حتى المستقبل، أو قد يراها أشخاص لم يعتقدوا أنهم قد يرونها.

المواضيع

تستخدم هذه الأنشطة أمثلة واقعية ومناقشات تحفّز الأطفال على التفكير لتعليمهم كيفية الحفاظ على إيجابية ملفهم الشخصي على الإنترنت من خلال إدارة خصوصيتهم وحماية معلوماتهم الشخصية.

- ✓ بناء سمعة إيجابية والحفاظ عليها في عالم الإنترنت وخارجه.
- ✓ احترام حدود خصوصية الآخرين، حتى لو كانت مختلفة عن حدودنا الشخصية.
- ✓ إدراك التأثيرات المحتملة للحضور الرقمي السلبي على الإنترنت..
- ✓ طلب المساعدة من شخص بالغ عند مواجهة المواقف الصعبة.

الأهداف بالنسبة للطلاب

معايير جمعية ISTE للمعلمين: 1a, 1b, 2a, 2c, 3b, 3c, 3d, 4b, 4d, 5a, 6a, 6b, 6d, 7a

معايير ISTE للطلاب 2016: 1c, 1d, 2a, 2b, 2d, 3b, 3d

معايير AASL للتعلّم: I.a.1, I.b.1, I.c.1, I.d.3, I.d.4, II.a.2, II.b.1, II.b.2, II.b.3, II.c.1, II.c.2, d.2., III.a.1, III.a.2, III.a.3, III.b.1,

III.c.1, III.c.2, III.d.1, III.d.2, IV.a.1, IV.a.2, V.a.2, VI.a.1, VI.a.2, VI.a.3

المعايير ذات الصلة

شارك بانتباه المفردات



الخصوصية على الإنترنت: مصطلح عام يعني عادةً القدرة على التحكم في المعلومات التي تشاركها على الإنترنت وفي من يمكنه رؤيتها ومشاركتها

البصمة الرقمية (أو الحضور الرقمي): بصمتك الرقمية هي جميع المعلومات المتوفرة عنك على الإنترنت، ويمكن أن تشمل الصور والفيديوهات والمقاطع الصوتية والنصوص و"الإعجابات" وتعليقاتك على الملفات الشخصية لأصدقائك. وتترك مشاركاتك على الإنترنت أثرًا مماثلًا لذلك الذي تتركه أقدامك عند المشي.

السمعة: تشمل الأفكار أو الآراء أو الانطباعات التي يكوّنها الآخرون عنك، والتي ترغب أن تكون إيجابية أو جيدة، رغم أنه لا يمكنك التأكد من ذلك.

المعلومات الشخصية: تُعرف المعلومات التي تُحدّد هوية الشخص، مثل الاسم وعنوان الشارع ورقم الهاتف ورقم التأمين الاجتماعي وعنوان البريد الإلكتروني، وغيرها بالمعلومات الشخصية (أو الحساسة). وينبغي التفكير مليًا قبل مشاركة هذا النوع من المعلومات على الإنترنت.

المبالغة في المشاركة: أي المبالغة في مشاركة المعلومات الشخصية في موقف معين أو محادثة على الإنترنت.

الإعدادات: وهو القسم في أي منتج رقمي أو تطبيق أو موقع ويب وما إلى ذلك حيث يمكنك تحديد أو تعديل ما تشاركه وكيفية التعامل مع حسابك، بما في ذلك إعدادات الخصوصية.

الحالات التي يجب عدم المشاركة فيها

يعمل الطلاب في فرق مكوّنة من فردين ويفكّرون في أسرار محتملة ويقارنون حدود الخصوصية في كل منها.

الأهداف بالنسبة للطلاب



- ✓ معرفة أنواع المعلومات الشخصية التي يجب الحفاظ على خصوصيتها.
- ✓ التذكير بضرورة احترام قرارات الآخرين المتعلقة بخصوصيتهم.

دعونا نتحدث



لماذا تعتبر الخصوصية مهمة؟

بصمتك الرقمية هي ما يمثلك على الإنترنت، وقد يعني هذا الصور والفيديوهات والمقاطع الصوتية والنصوص و"الإعجابات" وتعليقاتك على الملفات الشخصية لأصدقائك، وتمائل أهمية الحفاظ على حضور إيجابي على الإنترنت أهمية الحضور الإيجابي في العالم الفعلي، مثل المدرسة.

تُسهّل الإنترنت التواصل مع أفراد العائلة والأصدقاء والأشخاص الذين يشاركوك اهتماماتك. نحن نرسل رسائل ونشارك الصور وننضم إلى المحادثات على وسائل التواصل الاجتماعي بدون التفكير أحياناً في الأشخاص الآخرين الذين يمكنهم رؤيتها أيضاً. قد تصل الصورة أو المشاركة التي تعتقد أنها مضحكة وغير ضارة إلى أشخاص آخرين لم تعتقد أنهم سيرونها ويُسَاء فهمها من قبلهم الآن أو في المستقبل. وعند نشر مشاركة على الإنترنت، من الصعب محوها. تذكّر:

- يمكن رؤية بصمتك الرقمية مثل أي أمر آخر على الإنترنت من قبل أشخاص لم تلتق بهم مطلقاً.
- عندما ينتشر أمر ما عنك أو من قبلك على الإنترنت، فقد يظل عليها إلى الأبد. ويمكن تشبيه ذلك بقلم التأشير: حيث لا يمكنك أبداً محو ما كتبه حتى لو أدركت لاحقاً أنك لم تكن تقصده.

وهذا ما يجعل من خصوصيتك موضوعاً أساسياً. ويمكنك حمايتها من خلال عدم مشاركة إلا ما ترغب فعلاً بمشاركته واختيار ما تريد نشره أو مشاركته على الإنترنت بحذر. ما هي الأسباب الأخرى التي تجعل الخصوصية مهمة؟

من المهم أيضاً معرفة الحالات التي لا ينبغي فيها نشر مشاركة أو الرد على مشاركة شخص ما أو التعليق على صورته أو تعليقه أو مشاركة معلومات خاطئة. لقد سمعنا جميعاً جملة "فكر قبل النشر"، وهي بلا شك نصيحة جيدة. 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.

بعض الأسئلة لمتابعة النقاش (يمكن للطلاب أيضاً مناقشة هذه الأسئلة في البيت مع العائلة):

- متى يمكن مشاركة صورة أو فيديو يظهر فيه شخص آخر؟
- لماذا يصعب الاحتفاظ بالأسرار؟
- هل من المقبول في بعض الأحيان إفشاء سر شخص آخر؟
- ماذا لو نشر شخص يهكم أمره أمراً جعلك تشعر بأنه في خطر؟ إذا كنت تعتقد أنه يجب مشاركة هذا السر، هل ينبغي إبلاغه بأنك تفكر في ذلك قبل القيام بالأمر؟ هل يجب مشاركته مخاوفك؟

النشاط



1. تأليف سرّ

أولاً، يجب على الجميع تأليف سرّ غير حقيقي.

2. إخبار شريكك به

هل انتهيت من تأليف أسراركم؟ انقسموا الآن إلى فرق مكوّنة من فردين وليشارك كل منكم سرّه مع شريكه، وناقشوا الأسئلة الثلاثة التالية:

- هل تقبل بمشاركة هذا السرّ مع أي شخص؟
- مع من تقبل بمشاركة سرّك ولماذا؟
- ماذا سيكون شعورك إذا أفشى شخص ما سرّك للجميع دون إذن منك؟

3. مشاركة السرّ مع الصف

وأخيراً، يجب على كل طالب مشاركة السرّ الذي ألّفه مع الصف ووصف شعوره حيال مشاركته. يمكن للصف مناقشة إجاباتهم على الأسئلة الواردة أعلاه.

الخلاصة

الأسرار هي نوع واحد فقط من المعلومات الشخصية التي قد نرغب في الاحتفاظ بها أو مشاركتها فقط مع أفراد العائلة أو الأصدقاء المقربين. بعد مشاركة السر، لا يمكنك التحكم في كيفية ومدى انتشاره. ما هي أنواع المعلومات الأخرى التي يجب أن نحصر على حمايتها؟

- عنوان منزلك ورقم هاتفك
- عنوان بريدك الإلكتروني
- كلمات المرور الخاصة بك
- أسماء المستخدم الخاصة بك
- عملك الدراسي وغيره من الوثائق التي تنشئها

النشاط: لمن هذا الملف الشخصي؟

يدرس الطلاب مجموعة من المعلومات الشخصية حول شخصية وهمية من أجل محاولة استنتاج أمور عنها.

الأهداف بالنسبة للطلاب

- ✓ تحديد طرق للعثور على معلومات حول الأشخاص على الإنترنت.
- ✓ التفكير كيف يتم الحكم على شخص عندما يقوم بنشر مشاركات على الإنترنت.
- ✓ تحديد دقة المعلومات والفرق بين الافتراض والرأي والحقيقة.



دعونا نتحدث



ما هو مصدر المعلومات التي نعتقد أننا نعرفها؟

- هناك الكثير من المعلومات الشخصية التي يمكن العثور عليها على الإنترنت، وقد يجعلنا بعضها نكوّن آراءً أو افتراضات معيّنة حول أشخاص يتضح في ما بعد أنها خاطئة. في ما يلي الأسئلة التي سنقوم بمناقشتها:
- ما الذي يمكننا معرفته عن شخص ما من معلوماته الشخصية؟
- ما هي الافتراضات التي يمكننا أن نكوّن منها من المعلومات الشخصية، حتى لو لم نكن متأكدين؟
- هل نعرف كيف تم جمع هذه المعلومات في المقام الأول؟ كيف يمكننا تحديد المصدر؟

النشاط



1. التعرّف على الشخص

إذا قررت توزيع أوراق عمل للجميع، يجب أن يحصل كل طالب على نسخة للقراءة. إذا قرّرت العمل كمجموعة، اختر ثلاثة أشخاص وسجّل معلوماتهم الشخصية في قوائم كما في ورقة العمل، وتأكد من حصول كل طالب على نسخته الخاصة وقراءتها.

2. كتابة وصف

يتوزّع الطلاب إلى مجموعات، وتحصل كل مجموعة على إحدى الشخصيات وتكتب وصفاً سريعاً يجيب على السؤال التالي: "من هو هذا الشخص برأيك؟"

3. كشف الحقيقة

إليك الآن الحقيقة حول شخصياتنا (تذكّر عدم البدء بالقراءة حتى تنتهي كل المجموعات من كتابة الوصف):

- **سارة** هي طالبة في المدرسة الثانوية. وهي تخطط للانتحاق بالكلية العام المقبل حيث ترغب في دراسة الهندسة الكيميائية وتحلم بإنشاء شركتها الخاصة في المستقبل. مجالات اهتماماتها: العائلة والعمل التطوعي والثقافة الشعبية والموضة.
- **ليلي** هي لاعبة كرة سلة محترفة في فريق المدرسة الثانوية. تبلغ من العمر 15 عامًا وتعيش في عمان. لديها أخت تبلغ من العمر 8 سنوات. مجالات اهتماماتها: كرة السلة ودراسة الفن وعزف الغيتار وقضاء الوقت مع الأصدقاء.
- يبلغ عمر **فادي** 14 عامًا، وانضمّ مؤخرًا إلى فريق كرة القدم ولديه قطتان. وهو ماهر جدًا في الرسم ويحب قضاء عطلة نهاية الأسبوع في صنع الروبوتات. مجالات اهتماماته: التكنولوجيا وفريقه في كرة القدم والحيوانات وحقوقها.

4. النقاش

أي من الافتراضات كانت صحيحة، وأيها لم تكن كذلك؟ لماذا ولم لا؟ ماذا تعلمتم من هذا النشاط؟

المواد المطلوبة:

- مجموعات من عدة أنشطة خيالية أو حقيقية لأشخاص على الإنترنت. يمكنك توزيع ورقة العمل "لمن هذا الملف الشخصي؟" على كافة طلاب الصف أو لكل متعلم على حدة كواجب منزلي للمشاركة في اليوم التالي - اجمع الأمثلة باستخدام هذه الأفكار:
- حسابات وسائل التواصل الاجتماعي الخاصة بأفراد الأسرة أو المشاهير، إذا كان هذا مناسبًا لسن الطلاب
- سجّلات محفوظات المتصفح المطبوعة
- دفاتر أو أجهزة مناسبة لمهمة كتابة قصيرة

عند رؤيتنا لمشاركات وتعليقات وصور شخص معين، نحن نبني افتراضات عنه قد لا تكون صحيحة دائمًا، خاصةً إذا كنا لا نعرف هذا الشخص، وذلك لأن ما نراه على الإنترنت ليس سوى جزء من شخصيته واهتماماته. وقد يكون هذا الشخص لا يظهر شخصيته الحقيقية أو شارك شعورًا راوده فقط في لحظة نشره للمشاركة. لا يمكننا أن نعرف حقًا من هو أو كيف يشعر حتى نتعرف عليه شخصيًا. وحتى في تلك الحالة، تستغرق معرفته فعليًا بعض الوقت.


النشاط: لمن هذا الملف الشخصي؟

اقرأ كل مجموعة من أنشطة الأشخاص على الإنترنت أدناه. استنادًا إلى ما تراه هنا، اكتب وصفًا موجزًا عن هذا الشخص كما تتخيله، على سبيل المثال: ما الذي يعجبه وما لا يعجبه وما هي مجالات اهتماماته؟


فادي

Barney's Burger Emporium لقد ضيعنا هدف الفوز. هذا مؤسف!
على الأقل حاولنا.25 صورة لجراء حفلة ثانوية ويستفيلد الموسيقية اطلّعوا على موقع صديقي الإلكتروني!
لقد كتبت معظم الرموز البرمجية فيه.رقم قياسي جديد!
رائع. أنا أحب لعبة gem jam!

ليلي

لقد فزنا باللعبة! بقي لدينا لعبة واحدة قبل
الوصول إلى البطولة. عليّ التمرن أكثر على
تسديد الرميات الثلاثية.أنا أكره الحفلات الراقصة المدرسية.
#لن_أذهبكلية العلوم ، عمّان 10 علامات تدل على أن أهلك
يحاولون تدمير حياتك سأذهب في رحلة إلى البحر الميت مع
والدي هذا السبت سوف نقضي وقتًا رائعًاLa La Luna في منطقة مركز
المدينة 

سارة

صور من الحفل كأنها مأخوذة تحت الماء،
تبدون رائعين جميعًا!أفضل الطرق للتخلص من
البشرات أخي الصغير اليكس مزعج للغاية. ربما هو
كائن فضائيمخالفات سرعة مؤتمر المصممين الشباب في
جامعة تومبسون لقد شاهدت وأخيرًا فيلم SPY WARS
الجديد. روعة!

شارك بانتباه: النشاط 3

النشاط: كيف يرانا الآخرون؟

يستكشف الطلاب كيف تختلف نظرة مجموعات مختلفة من الأشخاص، مثل الأهل وأرباب الأعمال والأصدقاء والشرطة، إلى الشخصيات في النشاط السابق.

الأهداف بالنسبة للطلاب

- ✓ فهم وجهة نظر الأشخاص الآخرين بالنسبة لقراراتنا التي تتعلق بمشاركة المعلومات على الإنترنت.
- ✓ التفكير في عواقب كشف المعلومات الشخصية: ما تشاركه يصبح جزءاً من سمعتك ويمكن أن يدوم طويلاً.
- ✓ وضع هدف المحافظة على حضور إيجابي على الإنترنت بشكل مستمر.



دعونا نتحدث



وجهة نظر جديدة

قد تكشف المعلومات الموجودة في بصمتك الرقمية أكثر مما تريد كشفه للآخرين وقد تكون العواقب وخيمة.

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؟
- ما هي أنواع الأشخاص الذين قد (لا) يرغبون في رؤيتها؟
- كيف يمكن للآخرين رؤية هذه المعلومات؟
- كيف يمكن استخدام هذه المعلومات من قبل الآخرين؟

تختلف مستويات الخصوصية المطلوبة مع اختلاف المواقف. ويُعتبر التفكير في كيفية رؤية الآخرين لما تقوم بنشره من العادات الجيدة الأساسية فيما يتعلق بالخصوصية على الإنترنت.

النشاط



المواد المطلوبة:

- نسخة لكل طالب من الملفات الشخصية الوهمية من النشاط 2

1. لتأخذ وجهة نظر جديدة

سنتوزع الآن في مجموعات، وسوف تفكر كل مجموعة بالشخصية من وجهة نظر كل من المجموعات التالية:

- أحد الوالدين
- مدرس
- صديق
- رجل شرطة
- أنت بعد 10 سنوات
- صاحب العمل
- مُعلن

ما المهم بالنسبة لك بصفتك أحد الوالدين أو مديراً أو مدرِّباً أو صديقاً أو ما شابه ذلك؟ ما هي استنتاجاتك بشأن الشخصية؟ كيف ستستخدم هذه المعلومات؟ احذف المعلومات التي تعتقد أن الشخصية لن ترغب في أن تراها أنت.

2. عرض الاستنتاجات

تعرض كل مجموعة نتائجها وتشرح خياراتها المتعلقة بالخصوصية. إذا كان ذلك مناسباً لصفك الدراسي، قد تكون هذه فرصة جيدة نشاط للعب الأدوار.

3. مناقشة في الصف

ما هي أهم استنتاجاتك من نشاط المجموعة؟ 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؟

يمكن للأشخاص المختلفين رؤية نفس المعلومات واستخلاص استنتاجات مختلفة تمامًا. لا تفترض بأن الأشخاص على الإنترنت سيرونك بالطريقة التي تعتقد أنهم سيرونك بها.

شارك بانتباه: النشاط 4

الحفاظ على الخصوصية

يستعرض الصف أربعة سيناريوهات مكتوبة ويناقش أفضل حلول الخصوصية في كل واحد منها.

الأهداف بالنسبة للطلاب



- ✓ التعرف على كيفية رؤية مخاوف الخصوصية من وجهات نظر أشخاص مختلفين
- ✓ فهم كيف أن سيناريوهات مختلفة تستدعي مستويات مختلفة من الخصوصية.

دعونا نتحدث



سيناريوهات الخصوصية: ما الذي يجدر فعله؟

- السيناريو الأول:** تعرضت طفلة تعرفها في المدرسة للدغة حشرة غريبة سببت ظهور طفح جلدي متعدّد الألوان على بطنها. وهي لا تريد أن يعرف الآخرون ما حدث.
- هل يحق للآخرين أن يعرفوا؟
 - هل يجب أن تكون أنت من يخبرهم؟

السيناريو الثاني: يكتب شخص ما في مفكرته الشخصية. ينسخ شخص آخر ما كتبه وينشره على الإنترنت.

- هل كان تصرف الشخص الذي نشر المحتوى خاطئاً؟
- كيف سيكون شعورك إذا نشر شخص ما أمراً كنت تنوي الاحتفاظ به لنفسك؟

سيناريو 3: ينشر شخص على صفحة صديقك في إحدى وسائل التواصل الاجتماعي ما يلي: "أتمنى لك إجازة ممتعة".

- هل شارك الصديق بشكل علني خطته للذهاب في رحلة؟ وهل كان يريد أن يعرف الجميع بذلك؟
- هل هناك وسائل أكثر خصوصية لإيصال هذه الرسالة، كإرسال رسالة مباشرة أو رسالة نصية مثلاً؟

سيناريو 4: علمت بأن أحد الطلاب أنشأ حساباً مزيفاً على إحدى وسائل التواصل الاجتماعي منتحلاً شخصية طالب آخر بطريقة

- سلبية ومضماً معلوماته الشخصية.
- هل يحق للطالب أن يعرف؟
- هل يجب إبلاغ المعلم أو شخص بالغ موثوق به؟ كيف؟ وما الذي يمكن أن يحدث إذا لم يعرفوا؟
- ليس واضحاً من قام بإنشاء الحساب، ولكنك تعرف من فعل ذلك. هل يجب أن تعطي هذه المعلومات إلى شخص بالغ موثوق به؟

النشاط



سنستعرض أربعة سيناريوهات ونتحدث عن حل الخصوصية الخاص بكل منها. سنتوزع في أربع مجموعات بحيث تتولى كل مجموعة مناقشة سيناريو واحد، ونناقش بعد ذلك النتائج التي توصلنا إليها مع جميع طلاب الصف.

الخلاصة

يختلف السلوك والتصرفات المطلوبة باختلاف المواقف وذلك في عالم الإنترنت وخارجه. ومن المهم دائماً احترام خيارات الآخرين المتعلقة بالخصوصية، حتى لو كانت مختلفة عن خياراتنا.

شارك بانتباه: النشاط 5

"عالم الإنترنت" جبل المشاركة

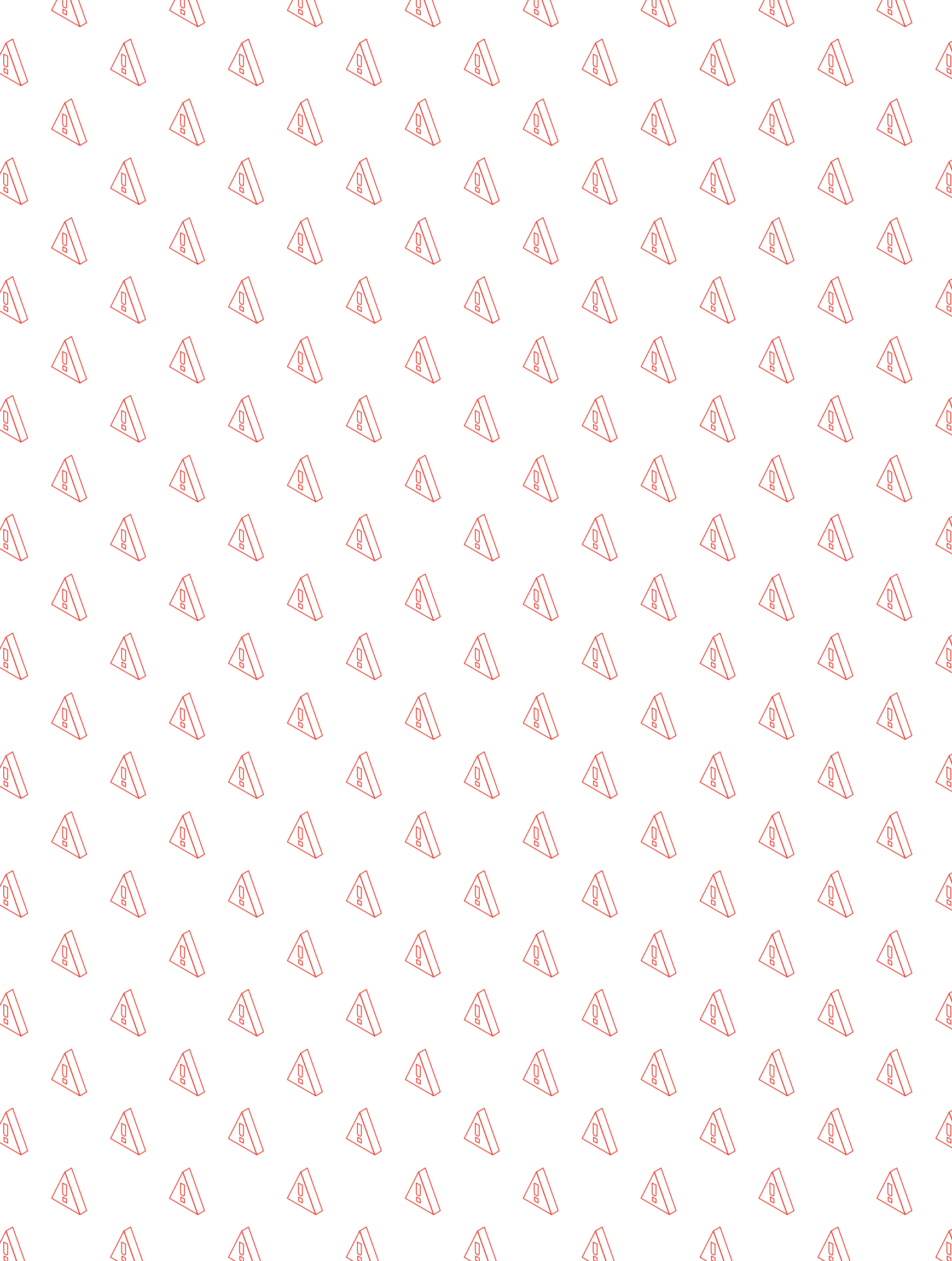
تُعتبر المنطقة الجبلية في مركز "عالم الإنترنت" نقطة التقاء للجميع. ولكن يجب أن تكون واعياً جداً لما تشاركه ومع من، لأن المعلومات تنتقل بسرعة كبيرة وقد يكون أحد معارفك ممن يبالغون في المشاركة.

افتح متصفح ويب على جهاز الكمبيوتر أو جهاز جوال (مثل الجهاز اللوحي)، وانتقل إلى g.co/abtalinternet

مواضيع النقاش



- اطلب من طلابك لعب مرحلة "جبل المشاركة" واستخدم الأسئلة التالية لتشجيع المزيد من النقاش حول الدروس المستفادة من اللعبة. يستفيد معظم الطلاب إلى أقصى حدّ إذا لعبوا بشكل فردي، ولكن يمكن أيضاً تقسيم الطلاب إلى فرق من لاعبين. وقد يستفيد الطلاب الأصغر سناً من ذلك بشكل خاص.
- من بين جميع المشاركات التي شاركتها في اللعبة، أي نوع تعتقد بأنك قد تشاركه عادةً في الواقع؟ ولماذا؟
 - صف لنا موقفاً تعرّضت له حيث شاركت أمراً عن طريق الخطأ ولم يكن ينبغي مشاركته.
 - برأيك، لماذا تم اختيار اسم "المُبالغ في المشاركة" للشخصية في "جبل المشاركة"؟
 - صف شخصية "المُبالغ في المشاركة" وكيفية تأثير تصرفاته على اللعبة.
 - هل تغيّرت طريقة تفكيرك حول مشاركة المعلومات مع الآخرين على الإنترنت بعد لعب "جبل المشاركة"؟
 - اذكر تصرّفاً مختلفاً ستلتزم به نتيجة ما تعلمته من هذه الدروس ومن اللعبة.
 - أعط مثالاً على نتيجة سلبية محتملة لمشاركة أمر بشكل علني بدلاً من إبقائه بين أصدقائك فقط؟
 - ما الخطوات التي يمكنك اتخاذها إذا شاركت أمراً شخصياً عن طريق الخطأ؟ وماذا لو شارك شخص ما أمراً شخصياً معك عن طريق الخطأ؟



لا تصدّق الخدع

تجنّب التصيّد الاحتيالي ومحاولات الاحتيال

- النشاط 1: لا تقع في فخ التصيّد الاحتيالي!
- النشاط 2: من أنت حقاً؟
- النشاط 3: حول الروبوتات
- النشاط 4: "عالم الإنترنت": نهر الحقيقة

نظرة عامة على الدرس

المواضيع

من المهم أن يفهم الأطفال أن المحتوى الذي يعثرون عليه على الإنترنت ليس بالضرورة صحيحاً أو موثوقاً، وقد يتضمن محاولات ضارة لسرقة معلوماتهم أو هويتهم. تشجّع عمليات التصيّد الاحتيالي وغيرها من عمليات الاحتيال على الإنترنت مستخدمي الإنترنت من جميع الأعمار على الاستجابة لاقتراحات من أشخاص لا يعرفونهم وأحياناً حتى من أشخاص ينتحلون هوية أشخاص يعرفونهم.

الأهداف بالنسبة للطلاب

- ✓ الإدراك بأن وجود أمر ما على الإنترنت ليس كفيلاً بضمان صحته
- ✓ معرفة كيف يحدث التصيّد الاحتيالي ولماذا يعتبر تهديداً، والخطوات التي يمكن اتخاذها لتجنبه
- ✓ اكتساب القدرة على تحديد مدى مصداقية مواقع الويب ومصادر المعلومات الأخرى وتوخي الحذر من التلاعب أو الادعاءات غير المثبتة أو العروض والجوائز المزوّرة وغيرها من عمليات الاحتيال على الإنترنت

المعايير ذات الصلة

- معايير ISTE للمعلمين: 1a, 2c, 3b, 3c, 4b, 5a, 6a, 6d, 7a
- معايير ISTE للطلاب لعام 2016: 1c, 2d, 2a, 3b, 3d, 7b, 7d
- معايير AASL للتعلّم: I.a.3, I.b.4, I.c.1, I.d.2, I.d.1, II.a.2, II.b.3, II.b.1, II.b.2, II.c.1, II.c.2, d.1., III.a.2, III.a.3, III.a.1, III.b.1, III.c.2, III.c.1, III.d.2, III.d.1, IV.a.2, IV.a.3, V.a.2, VI.a.1, VI.a.2, VI.a.3

لا تصدّق الخدع المفردات



الروبوت: يُسمى أيضًا "روبوت الدردشة" أو "المساعد الافتراضي"، وهو برنامج يعمل على الإنترنت أو على شبكة معيَّنة للإجابة تلقائيًا على الأسئلة أو لتنفيذ أوامر (مثل إعطاء اتجاهات الوصول إلى منزل صديقك الجديد) أو إنجاز مهام بسيطة (مثل تشغيل أغنية).

التصيّد الاحتيالي: محاولة لخداعك أو الاحتيال عليك لمشاركة معلومات تسجيل الدخول الخاصة بك أو معلوماتك الشخصية الأخرى على الإنترنت. يتم التصيّد الاحتيالي عادةً عن طريق البريد الإلكتروني أو الإعلانات أو مواقع شبيهة بأخرى اعتدت استخدامها.

التصيّد الاحتيالي الموجّه: محاولة تصيّد احتيالي تستهدفك أنت خصيصًا من خلال استخدام بعض معلوماتك الشخصية

محاولة الاحتيال: محاولة غير نزيهة لكسب المال أو أمر قيّم آخر من خلال خداع الأشخاص

شخص جدير بالثقة: هو شخص يمكنك الاعتماد عليه لاتخاذ الإجراء المناسب أو المطلوب

حقيقي: كل ما هو واقعي أو أصلي أو فعلي أو دقيق، أي أنه غير مزيف أو مقلّد

قابل للتحقق: ما يمكن إثباته أو إظهار صحته أو دقته

مضلل: أمر زائف أو إجراء أو رسالة تم تصميمها لخداع الأشخاص أو الاحتيال عليهم أو تضليل شخص ما

التلاعب: سيطرة شخص ما على شخص آخر أو وضع معين والتأثير عليه بشكل غير عادل أو غير شريف أو تحت التهديد. وقد يتم أيضًا التلاعب بالأمور التي تعثر عليها على الإنترنت، مثل صورة تم تعديلها لجعلك تصدق أمرًا غير حقيقي.

الاحتيال: محاولة خداع شخص ما للحصول على أمر قيّم منه

جدار الحماية: برنامج يحمي جهاز الكمبيوتر من معظم محاولات الاحتيال والخداع

ضار: كلمات أو أفعال تكون قاسية أو مؤذية. وقد تعني أيضًا البرامج الضارة التي تهدف إلى إلحاق الضرر بجهاز أو حساب الشخص أو معلوماته الشخصية.

انتحال الشخصية: إنشاء هوية أو حساب مزيف على إحدى وسائل التواصل الاجتماعي للاحتيال على الأشخاص ودفعهم إلى مشاركة معلوماتهم الشخصية أو الاعتقاد بأنهم يتحدثون إلى شخص حقيقي يملك حسابًا أو ملفًا شخصيًا أو صفحة حقيقية

محتوى اصطياد النقرات: محتوى أو مشاركات أو إعلانات مخادعة على الإنترنت تهدف إلى جذب انتباه الأشخاص وحملهم على النقر على رابط أو صفحة ويب، غالبًا لزيادة عدد المشاهدات أو الزيارات للموقع وكسب المال

لا تصدّق الخدع: النشاط 1

لا تقع في فخ التصيد الاحتيالي!

يلعب الطلاب لعبة يستعرضون خلالها عدّة رسائل إلكترونية ونصية ويحاولون تحديد الرسائل الحقيقية منها وتلك التي تعدّ محاولات تصيد احتيالي.

الأهداف بالنسبة للطلاب

- ✓ التعرف على الأساليب المستخدمة في سرقة الهويات
- ✓ مراجعة وسائل تساعد في تجنّب سرقة الهوية
- ✓ تشجيعهم على التحدث مع شخص بالغ موثوق به إذا كانوا يعتقدون بأنهم وقعوا ضحية لسرقة الهوية
- ✓ التعرف على الدلائل لوجود محاولة الخداع
- ✓ توخي الحذر في ما يتعلّق باختيار كيفية مشاركة معلوماتهم الشخصية والأشخاص الذين يمكن مشاركتها معهم



دعونا نتحدث



ما هو التصيد الاحتيالي؟

التصيد الاحتيالي هو عندما يحاول شخص ما سرقة معلومات مثل معلومات تسجيل الدخول أو الحساب الخاصة بك في بريد إلكتروني أو رسالة نصية أو أي اتصال على الإنترنت، من خلال التظاهر بأنه شخص تثق به. يمكن لرسائل التصيد الاحتيالي المرسلة بالبريد الإلكتروني والمواقع غير الآمنة التي يحاولون توجيهك إليها أو الملفات المرفقة التي يحاولون إقناعك بفتحها أيضًا زرع الفيروسات في جهاز الكمبيوتر الخاص بك. تستخدم بعض الفيروسات قائمة جهات الاتصال لاستهداف أصدقائك وأفراد عائلتك بنفس الطريقة، أو في هجوم احتيالي أكثر تخصيصًا. كما قد تحاول أشكال أخرى من عمليات الاحتيال خداعك لتنزيل برامج ضارة أو برامج غير مرغوب فيها من خلال إعلامك بوجود خطأ ما في جهازك. تذكر: لا يمكن لأي موقع ويب أو إعلان معرفة ما إذا كان هناك أي خطأ في جهازك!

تكون بعض محاولات التصيد الاحتيالي زائفة بوضوح. وقد يكون بعضها مخادعًا ومقنعًا، مثل عندما يرسل إليك الشخص المحتمل رسالة تتضمن بعض معلوماتك الشخصية. وهذا ما يسمى بالتصيد الاحتيالي الموجّه، وقد يكون من الصعب رصده لأن استخدام معلوماتك يجعل الأمر يبدو كما لو أن المرسل يعرفك حقًا.

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. في ما يلي بعض الأسئلة الممكنة:

- هل يبدو الموقع مهنيًا مثل مواقع الويب الأخرى التي تعرفها وتثق بها، وهل يتضمن شعار المنتج أو الشركة الأصلي ويخلو النص فيه من الأخطاء الإملائية؟
- هل يتوافق عنوان URL الخاص بالموقع مع اسم المنتج أو الشركة والمعلومات التي تبحث عنها؟ هل هناك أخطاء إملائية؟
- هل هناك أي نوافذ منبثقة غير مرغوب فيها؟
- هل يبدأ عنوان URL بـ <http://> ويظهر إلى يساره قفل أخضر صغير؟ (هذا يعني أن الاتصال آمن.)

- ماذا يرد في التفاصيل المطبوعة بخط صغير؟ (والتي تحوي عادةً التفاصيل الخادعة).
- هل يعرض البريد الإلكتروني أو الموقع أمرًا مشبوهًا، مثل فرصة كسب الكثير من المال؟ (عادةً ما تكون العروض جيدة جدًا لحد يصعب تصديقها).
- هل يساورك شعور غريب تجاه الرسالة؟ كما لو أنهم يعرفونك، ولكنك لست متأكدًا تمامًا؟

وماذا لو وقعت ضحية عملية احتيال؟ القاعدة الأولى: لا داعي للذعر!

- أخبر والدك أو معلمك أو أي شخص بالغ تثق به على الفور. فكلما أطلت الانتظار، زادت النتائج سوءًا.
- غير كلمات مرور حساباتك على الإنترنت.
- إذا وقعت ضحية لعملية احتيال، أخبر أصدقاءك والأشخاص في جهات الاتصال الخاصة بك على الفور لأنه قد يتم استهدافهم بعدك.
- استخدم الإعدادات للإبلاغ عن الرسالة كرسالة غير مرغوب فيها، إن أمكن.

النشاط



المواد المطلوبة:

- مستند ورقة العمل "أمثلة على التصيد الاحتيالي" يتم توزيعه على الطلاب

أجوبة ورقة العمل "أمثلة على التصيد الاحتيالي"

- 1. حقيقي.** تطلب الرسالة الإلكترونية من المستخدم الانتقال إلى موقع الشركة على الويب وتسجيل الدخول إلى حسابه بنفسه، بدلاً من تقديم رابط في الرسالة الإلكترونية أو طلب إرسال كلمة المرور عبر البريد الإلكتروني (قد تنقل الروابط المستخدمين إلى مواقع ويب ضارة).
- 2. مزيف.** عنوان URL مشبوه وغير آمن
- 3. حقيقي.** لاحظ وجود `https://` في عنوان URL.
- 4. مزيف.** عرض مشبوه مقابل الحصول على تفاصيل البنك
- 5. مزيف.** عنوان URL غير آمن ومشبوه

1. تدرس المجموعات الأمثلة

لنتوزع في مجموعات، ولتدرس كل مجموعة هذه الأمثلة عن رسائل ومواقع ويب.

2. يحدّد كل طالب خيارًا

حدّد صفة كل مثال "حقيقي" أم "مزيف" وشرح أسباب الخيار.

3. تناقش المجموعات الخيارات

أي من الأمثلة بدت جدية بالثقة وأيها بدت مشبوهة؟ هل فاجأتك إحدى الإجابات؟ إذا كان الجواب نعم، اشرح السبب.

4. مزيد من المناقشة

في ما يلي بعض الأسئلة التي تساعدك على تقييم الرسائل والمواقع التي تجدها على الإنترنت:

• هل تبدو هذه الرسالة صحيحة؟

ما هو حدسك الأول؟ هل تلاحظ أي أجزاء مشبوهة؟ هل تعرض عليك إصلاح مشكلة أنت لا تعرف بوجودها؟

• هل تُقدّم لك هذه الرسالة الإلكترونية عرضًا مجانيًا؟

تكون العروض المجانية عادةً غير حقيقية.

• 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 "اختبارات الشخصية" إلى جمع حقائق تسهّل توقيع كلمة المرور الخاصة بك أو غيرها من المعلومات السرية. والجدير بالذكر أن 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 تعرّضك أنت والآخرين للخطر. لا ترسلها إلا إذا كنت واثقًا من المصدر ومن أن الرسالة آمنة.

• هل هناك تفاصيل مكتوبة بخط صغير؟

ستجد في أسفل معظم المستندات تفاصيل مكتوبة بخط صغير. ويحتوي النص غالبًا على معلومات يُفترض أن تفوتك. على سبيل المثال، قد يشير العنوان في الأعلى إلى حصولك على هاتف مجاني، ولكن في التفاصيل المكتوبة بخط صغير ستقرأ أنه عليك دفع 200 دولار شهريًا لهذه الشركة. وتنبّه إلى أن غياب هذه التفاصيل مثير للشبهات بنفس القدر.

ملاحظة: لأغراض هذا التمرين، افترض بأن خدمة "بريد مستخدم الإنترنت" حقيقية وموثوق بها.

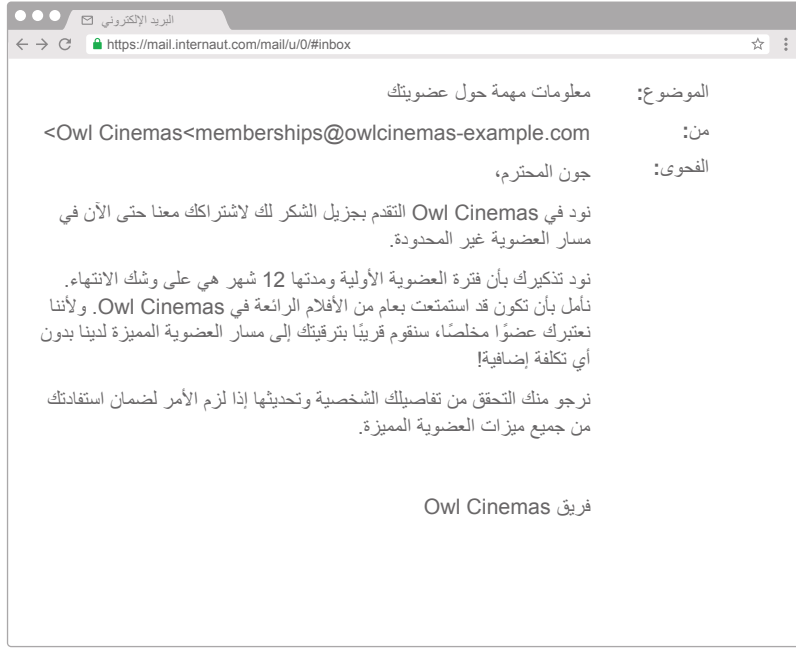
الخلاصة

عندما تكون متصلاً بالإنترنت، تنبّه دومًا لمحاولات التصيّد الاحتيالي في بريدك الإلكتروني والرسائل النصية والرسائل المنشورة؛ وإذا وقعت ضحية لمثل هذه المحاولات، احرص على إبلاغ شخص بالغ تثق به على الفور.

ورقة عمل: النشاط 1

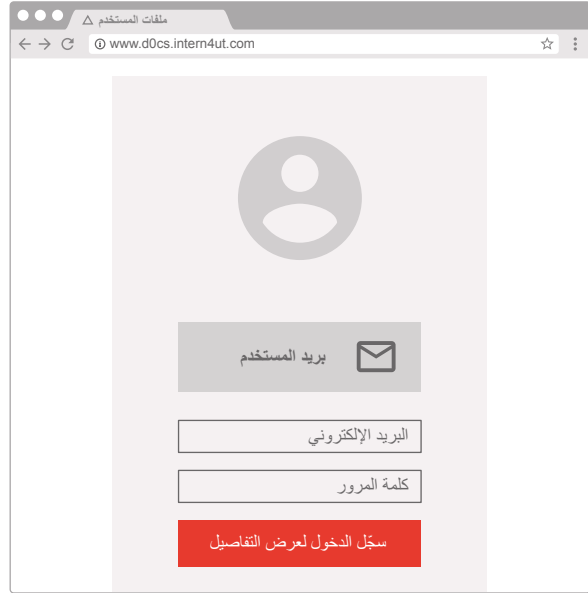
أمثلة على التصيد الاحتيالي

1. هل هذا حقيقي أم مزيف؟



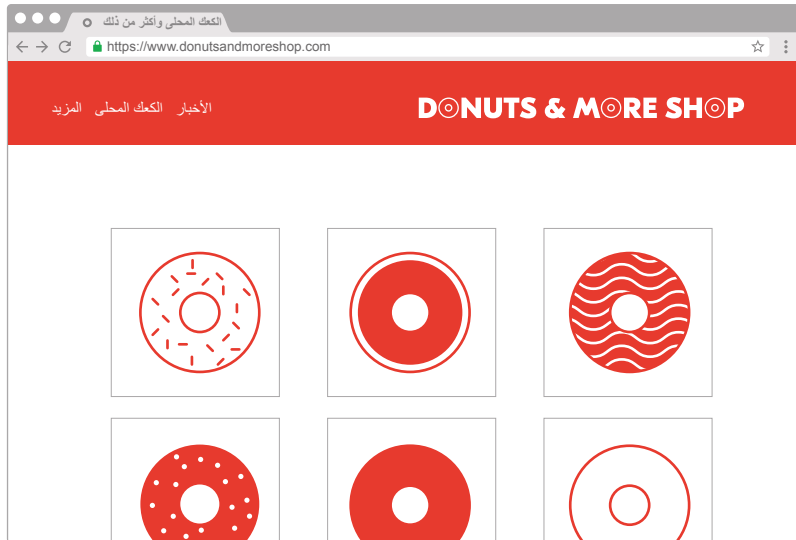
مزيف. حقيقي.

2. هل هذا حقيقي أم مزيف؟



مزيف. حقيقي.

3. هل هذا حقيقي أم مزيف؟



مزيف. حقيقي.

4. هل هذا حقيقي أم مزيف؟

حقيقي.

مزيف.

البريد الإلكتروني

https://internaui.mail.com/mail/u/0/#inbox

فرصة رائعة

الموضوع: <Robin<robin@robin-hood-example.com

من: الصديق المحترم.

الفحوى: اسمي روبن وأنا معلم من مدينة نوتنغهام. أنا أدرس عددًا كبيرًا جدًا من الطلاب وأؤمن بأنني أصنع تغييرًا كبيرًا في حياة هؤلاء الأطفال. لسوء الحظ، يقوم مأمور المدينة بفرض ضرائب باهظة عليّ. وكما تعلم، ليس من المفروض على المعلمين دفع مثل هذه الضرائب المرتفعة لأننا لا نحصل على أجور عالية. أنا على وشك أن أرتب مبلغًا كبيرًا من المال (أكثر من 5 ملايين دولار) ولا أريد أن يعلم المأمور بهذا الأمر.

لقد كنت دائمًا ناعم الصديق ولذلك أرغب في ايداع الأموال في حسابك المصرفي حتى انقضاء فترة الضريبة.

وكمكافأة لك، أنا على استعداد لترك مبلغ مليون دولار في حسابك. هذه صفقة جيدة وأنا أعرضها عليك أنت فقط. أرسل لي لو سمحت تفاصيل حسابك المصرفي الكاملة حتى أتمكن من ايداع هذه الأموال فيه.

صديقك الوفي إلى الأبد،
روبين لوكسلي

5. هل هذا حقيقي أم مزيف؟

حقيقي.

مزيف.

خدمة حسابات المستخدم

http://www.internautaccounts.com-genuine-login.com/

حسابات المستخدمين

مهلاً، هل هذا حقًا أنت؟

يبدو أنك تحاول تسجيل الدخول إلى حسابك من موقع جديد. فقط بهدف التأكد بأنك أنت من تقوم بذلك وأن هذه ليست محاولة لاختراق حسابك، الرجاء إكمال عملية إثبات الملكية السريعة التالية. مزيد من المعلومات عن هذا التدبير الأمني الإضافي.

اختر طريقة إثبات الملكية

تأكيد رقم الهاتف

أدخل رقم الهاتف الكامل

ستقوم خدمة بريد المستخدم بالتحقق إذا كان هذا هو نفس رقم الهاتف المسجل لدينا - لن نرسل لك أي رسائل.

تأكيد عنوان البريد الإلكتروني لاسترداد الحساب:

أدخل عنوان البريد الإلكتروني الكامل

ستقوم خدمة بريد المستخدمين بالتحقق إذا كان هذا هو نفس عنوان البريد الإلكتروني المسجل لدينا - لن نرسل لك أي رسائل.

متابعة

لا تصدّق الخدع: النشاط 2 من أنت حقاً؟

يتمرن الطلاب على مهارات مكافحة التصيد الاحتيالي بطريقة تفاعلية ويناقدون الاستجابات المحتملة للنصوص والمشاركات وطلبات الصداقة والصور والرسائل الإلكترونية المشبوهة.

الأهداف بالنسبة للطلاب

- ✓ إدراك أن بعض الأشخاص على الإنترنت قد يدعون أموراً غير صحيحة عن أنفسهم
- ✓ التأكد من صحة هوية الشخص قبل الرد
- ✓ طرح الأسئلة أو طلب المساعدة من شخص بالغ إذا كان من الصعب تحديد هوية الشخص



دعونا نتحدث



كيف تتأكد من صحة هويتهم؟

عندما تتحدث هاتفياً مع صديقك، يمكنك التأكد من هويته من خلال صوته على الرغم من أنك لا تستطيع رؤيته. ولكن تختلف الأمور في عالم الإنترنت، حيث أحياناً يصعب التأكد من صحة ادّعاءات شخص ما. ففي التطبيقات والألعاب، يتظاهر الأشخاص أحياناً بأنهم أشخاص آخرون على سبيل الدعابة أو بهدف العبث. وفي بعض الحالات، ينتحلون صفة أشخاص آخرين بهدف سرقة معلومات شخصية خاصة. وقد يطلب شخص غريب التواصل معك أثناء استخدامك للإنترنت. والأفضل في هذه الحالة عدم الرد أو إخبار أحد الوالدين أو شخص بالغ تثق به بأنك لا تعرف الشخص الذي يحاول التواصل معك. وإذا قررت الرد، من المستحسن أن تحاول أولاً اكتشاف ما يمكنك معرفته عن الشخص. تحقق من ملفه الشخصي وقائمة أصدقائه أو ابحث عن معلومات أخرى تؤكد هويته.

هناك طرق متعددة للتحقق من هوية شخص ما على الإنترنت. وفي ما يلي بعض الأمثلة.

ملاحظة للمعلم

يمكن إجراء عصف ذهني في الصف حول السؤال "كيف يمكننا التحقق من هوية شخص ما على الإنترنت؟" أولاً؛ ثم متابعة المحادثة بالاستناد إلى هذه الأفكار الأولية.

• هل تبدو الصورة في ملفهم الشخصي مشبوهة؟

هل صورة الملف الشخصي غير واضحة أو يصعب رؤيتها؟ أو لا يوجد صورة على الإطلاق، وبدلاً من ذلك هناك رمز تعبيرى أو صورة شخصية من الرسوم المتحركة؟ تُسهل الصور غير الواضحة والرموز التعبيرية وصور الحيوانات الأليفة وما شابه ذلك على الشخص إخفاء هويته في وسائل التواصل الاجتماعي. ومن الشائع أيضاً قيام المحتالين بسرقة صور شخص حقيقي من أجل إنشاء ملف شخصي مزيف وانتحال شخصيته. هل يمكنك العثور على المزيد من الصور للشخص الذي يحمل الحساب اسمه؟

• هل يحتوي اسم المستخدم الخاص بهم على اسمهم الحقيقي؟

هل يتوافق اسم المستخدم مع الاسم الحقيقي على وسائل التواصل الاجتماعي مثلاً؟ (على سبيل المثال، يحتوي الملف الشخصي لجين دو على عنوان URL مثل SocialMedia.com/jane_doe).

• هل هناك سيرة ذاتية في الملف الشخصي؟

إذا كان الجواب نعم، هل تبدو وكأن شخصاً حقيقياً قام بكتابتها؟ قد لا تحتوي الحسابات المزيفة على الكثير من المعلومات عن الشخص أو قد يتم نسخ مجموعة من المعلومات أو تجميعها بشكل عشوائي لإنشاء ملف شخصي مزيف. هل هناك أي تفاصيل في سيرتهم الذاتية يمكنك تأكيدها من خلال البحث عنها؟

• كم من الوقت مضى على نشاط هذا الحساب؟ هل يلائم النشاط الذي تراه توقعاتك؟

هل الملف الشخصي جديد أم يظهر فيه الكثير من النشاط؟ هل هناك أصدقاء مشتركين معك؟ لا تحتوي الحسابات المزيفة عادةً على الكثير من المحتوى أو دلائل على مشاركات وتعليقات وأي تواصل مع أشخاص آخرين.

النشاط



المواد المطلوبة:

- نسخة من ورقة العمل "من أنت حقًا؟" مقسّمة إلى شرائط ويحوى كل منها سيناريو واحد
- وعاء أو صندوق توضع فيه الشرائط (تختار كل مجموعة من الطلاب شريطة واحدة)
- ورقة إجابات التصيّد الاحتيالي

1. تراجع المجموعات السيناريوهات

ستوزع الآن في مجموعات. وستختار كل مجموعة سيناريو وتحدث عن كيفية التصرف في مثل هذا الموقف.

2. تمثل المجموعات السيناريوهات

تقوم كل مجموعة بتمثيل السيناريو الخاص بها: طالب يؤدي دور الراوي، وطالب ثاني يمثّل "الرسالة"، وثالث يرد، وربما طالب رابع يشرح خيارات المجموعة.

3. يناقش جميع الطلاب خيارات المجموعات

وأخيرًا، لنستخدم ورقة الإجابات هذه لمناقشة خيارات كل مجموعة. لا تترددوا في كتابة المزيد من الرسائل التي تعتقدون بأن كشفها سيكون أكثر تعقيدًا. وعلى كل مجموعة مشاركة الرسائل التي كتبتها مع المجموعات الأخرى.

أنت تقرر مع من تتحدث على الإنترنت. تأكد من هوية الأشخاص الذين تتواصل معهم!

الخلاصة

من أنت حقًا؟

السيناريو الأول

يصلك طلب متابعة على الإنترنت من شخص غريب. "مرحبًا! تبدو كأنك شخص ممتع. دعنا نمضي بعض الوقت الممتع سوياً! هل يمكنك متابعتي؟ - سامر"

السيناريو الثاني

تصلك رسالة نصية على هاتفك الجوال من شخص لا تعرفه. "مرحبًا، أنا ياسمين! هل تتذكرني من الصيف الماضي؟"

السيناريو الثالث

تصلك رسالة من شخص لا تتبعه. "مرحبًا! أحب مشاركاتك، أنت مضحك جدًا! أعطني رقم هاتفك ويمكننا التحدث أكثر! "

السيناريو الرابع

يصلك طلب درشة من شخص لا تعرفه. "لقد رأيتك في القاعة اليوم. أنت وسيم للغاية! ما هو عنوانك؟ يمكنني الحضور وقضاء الوقت سوياً."

السيناريو الخامس

تصلك رسالة على الإنترنت. "مرحبًا، لقد التقيت صديقتك زينة! لقد حدثتني عنك وأرغب في لقائك. أين تسكن؟"

من أنت حقًا؟

في ما يلي خمسة سيناريوهات للرسائل التي قد يتلقاها أي شخص على الإنترنت أو الهاتف. ولكل منها قائمة من طرق رد مقترحة بعضها جيّدة والأخرى غير محبّدة. اختّر تلك التي تجدها مناسبة أو اقترح طرقًا أخرى. إذا حدث أحد هذه السيناريوهات في الواقع ولم تكن متأكدًا مما يجب فعله، يكون عدم الرد أسهل ردّ. يمكنك دائمًا التجاهل أو الحظر. ولا ضير أبدًا في التحدث إلى أحد الوالدين أو المعلم حول هذا الموضوع.

السيناريو الأول

تصلك رسالة من شخص لا تعرفه: "مرحبًا! تبدو كأنك شخص ممتع. دعنا نمضي بعض الوقت الممتع سوياً! هل يمكنك إضافتي إلى قائمة أصدقائك؟ - سامر" ماذا تفعل؟

• **تجاهل سامر.** إذا كنت لا تعرفه، يمكنك ببساطة أن تقرر عدم التحدث معه.

• **أهلاً سامر. هل أعرفك؟** إذا كنت غير متأكد، اسأل أولاً.

• **تحظر سامر.** إذا قررت بعد أن تحققت من هويته حظه، لن تصلك أي رسائل أخرى منه. وعلى معظم مواقع التواصل الاجتماعي، لن يعلم أنك حظرت.

• **تحقق من ملف سامر الشخصي.** كن حذرًا لأنه من السهل إنشاء الملفات الشخصية المزيفة! تحقق من قائمة أصدقاء هذا الشخص ودائرة معارفه. قد تكون دائرة معارفه طريقة أخرى لمعرفة ما إذا كان شخصًا حقيقيًا، خاصة إذا لم يكن بينكما أصدقاء مشتركين. إذا لم يكن هناك الكثير من النشاط في صفحته، فذلك مؤشر آخر على أنه غير حقيقي.

• **تضيف سامر إلى قائمة أصدقائك** إذا بدا شخصًا حقيقيًا. لا يُنصح بهذا إلا إذا تحققت من هويته واستشرت شخصًا بالغًا تثق به.

• **تشارك معه معلومات شخصية.** لا تشارك معلومات شخصية مع الأشخاص الذين لا تعرفهم.

السيناريو الثاني

تصلك رسالة نصية على هاتفك الجوال من شخص لا تعرفه. "مرحبًا، أنا ياسمين! هل تتذكرني من الصيف الماضي؟" ماذا تفعل؟

• **تحظر ياسمين.** قد يبدو هذا تصرفًا فطريًا إذا كنت تعرفها فعلاً. ولكن إذا كنت متأكدًا من أنك لم تلتق بأي شخص يدعى ياسمين في الصيف الماضي أو إذا كانت ترسل لك الكثير من الرسائل وتبالغ في المشاركة عن نفسها، يكون من الأفضل حظرها.

• **تجاهل ياسمين.** إذا كنت لا تعرف هذا الشخص، يمكنك ببساطة عدم الرد.

• **أهلاً ياسمين. هل أعرفك؟** يعد هذا خيارًا آمنًا إذا لم تكن متأكدًا من مقابلتك لها في السابق وتريد معرفة ذلك من خلال اكتشاف المزيد. لكن لا تخبر ياسمين أين كنت خلال الصيف الماضي!

• **"أنا لا أتذكرك ولكن بإمكاننا اللقاء."** هذه ليست فكرة جيدة. لا تقابل إطلاقًا شخصًا لا تعرفه.

السيناريو الثالث

تصلك رسالة مباشرة من @soccergirl12، وهو شخص لا تتبعه. "مرحبًا! أحب مشاركاتك، أنت مضحك! أعطني رقم هاتفك ويمكننا التحدث أكثر!" ماذا تفعل؟

• **تجاهل @soccergirl12** ليس عليك الرد إذا كنت لا تريد ذلك.

• **تحظر @soccergirl12** إذا شعرت بأن هذا الشخص مشبوه وخطره، لن تصلك منه أي رسائل أخرى مطلقًا؛ إلا إذا أنشأ ملفًا شخصيًا مزيّفًا جديدًا وتواصل معك عن طريقه.

• **"أهلاً، هل أعرفك؟"** إذا لم تكن متأكدًا، الأفضل أن تستفسر قبل إعطاء معلومات شخصية مثل هاتفك.

• **"حسنًا، رقمي هو..."** كلا! حتى لو تحققت من هوية هذا الشخص، لا يوصى بمشاركة معلومات شخصية على وسائل التواصل الاجتماعي. يمكنك إيجاد طريقة أخرى للتواصل، من خلال الأهل أو المعلمين أو شخص آخر تثق به.

السيناريو الرابع

يصلك طلب دردشة من شخص لا تعرفه. "لقد رأيتك في القاعة اليوم، أنت وسيم للغاية! ما هو عنوانك؟ يمكننا أن نقضي وقتًا ممتعًا سوياً." ماذا تفعل؟

• **تجاهل الطلب.** قد يكون هذا خيار جيد.

• **تحظر هذا الشخص.** لا تتردد إذا لم تشعر بالارتياح تجاه هذا الشخص.

• **"من أنت؟"** من المفضل ألا تفعل ذلك، إذا بدت الرسالة سطحية، من الأفضل عدم الإجابة أو حظر الشخص.

• **"هل هذه أنت يا ليلي؟ أنت جميلة أيضًا! أنا أسكن في 240 شارع الأزهر."** هذه ليست فكرة جيدة، حتى لو كنت تعتقد أنك تعرف الشخص. قبل أن تعطي عنوانك أو أي معلومات شخصية أخرى لأي شخص، تحقق من هويته حتى لو كنت تعتقد أنك تعرفه. لا تلتقي بشخص تعرفه فقط من خلال التواصل على الإنترنت.

السيناريو الخامس

وصلتك هذه الرسالة: "مرحبًا، قابلت صديقتك زينة! لقد حدثني عنك وأرغب في لقائك. أين تسكن؟" ماذا تفعل؟

- **تجاهل الرسالة.** إذا لم تكن تعرف هذا الشخص ولكن لديك صديقة تدعى زينة، أفضل ما يمكن فعله هو التحقق من زينة أولاً قبل الرد على هذه الرسالة.
- **تحظر المُربيل.** 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 تكن تعرف هذا الشخص، من الأفضل عدم الرد، على الأقل حتى تستفسر من زينة.

يتفاعل الطلاب بشكل متزايد مع "أصوات" غير بشرية التي تصدر من الأجهزة والتطبيقات والمواقع هذه الأيام - معظمها في المنزل، ولكنها تتزايد في المدرسة أيضاً. ويُطلق على هذه الأصوات أحياناً اسم "روبوتات الدردشة" وفي أحيان أخرى "مساعدين افتراضيين"، وغالباً ما يُشار إليها بالروبوتات فقط. يتألف النشاط هذا من أسئلة وأجوبة فقط وهو مصمّم لتشجيع الطلاب على مناقشة أفكارهم في ما يتعلّق بالتفاعل مع الروبوتات.

ملاحظة: حاول أن تُبقي باب المناقشة مفتوحاً، حيث تم تصميم هذا النشاط لتشجيع التفكير النقدي، وليس لتقديم أي استنتاجات.

الأهداف بالنسبة للطلاب

- ✓ التعرّف على هذه التكنولوجيا التفاعلية التي تظهر بشكل متزايد في حياة الطلاب
- ✓ التعرّف على أنواع مختلفة من الروبوتات
- ✓ تحليل تأثير هذه التكنولوجيا الإيجابي والسلبي على الحياة اليومية



دعونا نتحدث



يتزايد استخدام الأشخاص للروبوتات في الوقت الحاضر. هل سبق أن سمعت هذه الكلمة من قبل؟ يطلق عليها بعض الأشخاص اسم "روبوتات الدردشة" أو "مساعدين افتراضيين". ويتم استخدامها في العديد من الأغراض مثل اللعب ومعرفة حالة الطقس والإجابة على الأسئلة والحصول على الاتجاهات وضبط المؤقت وما إلى ذلك. وفي بعض الأحيان يُطلق عليها اسم بشري، وأحياناً تصف أسماؤهم ما يفعلونه، مثل "Dog a Day"، وهو روبوت يرسل صورة كلب كل يوم. يمكن استخدام الروبوتات على الأجهزة الجوّالة أو على الإنترنت أو في السيارات، أو قد تكون أجهزة خاصة يحتفظ بها الأشخاص في غرف مختلفة من منازلهم. دعونا نتحدث عن تجربة الصف مع الروبوتات. في ما يلي بعض الأسئلة التي يمكن طرحها:

- هل تعرف ما هو الروبوت؟
- كم شخص بينكم سبق له التحدث إلى روبوت؟ على أي نوع من الأجهزة؟
- من يرغب في مشاركة تجربته معنا؟
- ما الوظائف التي تبرع برأيك الروبوتات في تأديتها (أمثلة يمكن عرضها: السؤال عن حالة الطقس أو الاطلاع على آخر الأخبار أو الألعاب أو الحصول على معلومات)؟
- تستخدم الروبوتات ما يُسمى بالذكاء الاصطناعي. يعمل الذكاء الاصطناعي على مبدأ التعلّم من أسئلتك حتى يتمكن من مساعدتك بشكل أفضل. للقيام بذلك، "تتذكر" الروبوتات في بعض الأحيان أو تسجّل ما تطلبه منها أو تقوله لها. هل يجعلك هذا تفكر في ما قد تقوله لروبوت؟ ما الذي يمكن أن تقوله وما نوع المعلومات التي ستحتفظ بها لنفسك؟
- هل تعتقد أنه يشبه التحدث إلى إنسان؟ ما هي أوجه التشابه والاختلاف؟
- كيف يتعامل الأشخاص الذين تعرفهم أو يتحدثون مع روبوتات؟
- كيف قد تتحدث أنت معه؟ هل تكون لطيفاً، أم تصرخ عليه أحياناً؟
- هل يعد الصراخ على الروبوتات أمراً مقبولاً؟ لماذا و لم لا؟ (هل يشبه هذا ممارسة نوع معين من التفاعل)؟
- يعتقد بعض الأطفال الصغار أحياناً أن الروبوتات هي كائنات بشرية. ما الذي يمكنك قوله لأختك الصغيرة أو أخيك أو قريبك لمساعدتهم في فهم مع من يتحدثون؟
- إذا كان بإمكان الروبوتات أن تتعلم من البشر، هل هناك أمر لن تقوله لأنك لا تريد أن يعرفه الروبوت الخاص بك؟ (تلميح: تذكر مرة أخرى في أنشطة "شارك بانتباه" وتحدث عن علاقتها بهذه النقطة).
- هل يمكن تصنيف المعلومات على أنها "جيدة أو سيئة" أو "حقيقية أو مزيفة"؟ كيف يمكننا محاولة الإجابة على هذه الأسئلة؟

النشاط



بعد المناقشة المشتركة في الصف أو في مجموعات حول الأجهزة في غرفة الصف، ابحث عن صور لروبوتات ومعلومات (بما في ذلك مقالات إخبارية) عنها. قد تتضمن مصطلحات البحث "روبوتات" أو "روبوتات الدردشة"، أو "مساعدين افتراضيين". قررُوا سوياً في الصف إذا كانت المعلومات جيدة واطلب من الطلاب اختيار مقال واحد لأخذه إلى المنزل وقراءته مع الأهل وكتابة ملخص من فقرة واحدة عنه.

الخلاصة

يُعد التفكير النقدي أحد أفضل الأدوات التي نملكها للاستمرار في تعزيز الاستخدام الإيجابي للتكنولوجيا، وأروع ما في الأمر هو أنها أداة التي تتحسن كلما زاد استخدامها. التعبير عن الأفكار ومشاركتها مع الآخرين هو وسيلة قوية وممتعة لاستخدام هذه الأداة وتحسينها.

لا تصدّق الخدع: النشاط 4

"عالم الإنترنت": نهر الحقيقة

يحمل النهر الذي يمرّ في "عالم الإنترنت" حقيقةً وخيالاً. لكن الأمور ليست دائماً كما تبدو. اجتز المنحدرات بالاعتماد على معرفتك واحترس من المخادعين المرابطين في الماء الذين سيحاولون خداعك.

افتح متصفح ويب على جهاز الكمبيوتر أو جهاز جوّال (مثل الجهاز اللوحي)، وانتقل إلى g.co/RealityRiver

مواضيع النقاش



- اطلب من طلابك لعب مرحلة "نهر الحقيقة" واستخدم الأسئلة التالية لتشجيع النقاش حول الدروس المستقاة في اللعبة. يستفيد معظم الطلاب إلى أقصى حدّ إذا لعبوا بشكل فردي، ولكن يمكن أيضاً تقسيم الطلاب إلى فرق من لاعبين. وقد يستفيد الطلاب الأصغر سناً من ذلك بشكل خاص.
- أعط مثلاً لموقف كان عليك فيه تحديد ما إذا كان أمر ما على الإنترنت حقيقيّاً أو مزيفاً. ما هي العلامات التي لاحظتها؟
 - من هو المُتصيّد الاحتيالي؟ صف سلوكه وكيف يؤثر على اللعبة.
 - هل أدى لعب نهر الحقيقة إلى تغيير الطريقة التي ستقيّم بها المعلومات والأشخاص على الإنترنت في المستقبل؟ إذا كان الجواب نعم، كيف سيحدث ذلك؟
 - أعط مثلاً عن تصرّف مختلف ستلتزم به بعد ما تعلّمته من هذه الدروس واللعبة.
 - ما هي العلامات التي يمكن أن تشير إلى أن أمراً يبدو مشبوهاً أو مريباً على الإنترنت؟
 - ما هو شعورك عندما تصادف شيئاً مشبوهاً على الإنترنت؟
 - إذا كنت غير متأكد من صحة أمر ما، ماذا يجب أن تفعل؟

ملاحظات



احم أسرارك

إدراك أهمية الخصوصية والأمان

نظرة عامة على الدرس

- النشاط 1: كيف تختار كلمة مرور قوية
- النشاط 2: كيف تحتفظ بها لنفسك
- النشاط 3: "عالم الإنترنت": قلعة الأمان

المواضيع

لا تتوفر دائمًا حلول صحيحة وخاطئة واضحة لمسائل الخصوصية والأمان على الإنترنت. فحماية معلوماتك الشخصية والخاصة وكل المعلومات التي تخصك وحدك تتطلب طرح الأسئلة الصحيحة والعتور على الإجابات الملائمة لك.

الأهداف بالنسبة للطلاب

- ✓ التعرف على أهمية الخصوصية وصلتها بالأمان على الإنترنت
- ✓ التمرن على إنشاء كلمات مرور قوية
- ✓ مراجعة الأدوات والإعدادات التي تحمي من المخترقين والتهديدات الأخرى

المعايير ذات الصلة

- معايير ISTE للمعلمين: 1a, 2c, 3b, 3c, 3d, 4b, 6a, 6d, 7a
- معايير ISTE للطلاب لعام 2016: 1c, 1d, 2b, 2d, 3d, 6a
- معايير AASL التعليمية: 1.d.1, 1.d.2, 1.d.3, 1.d.4, 1.d.5, 1.d.6, 1.d.7, 1.d.8, 1.d.9, 1.d.10, 1.d.11, 1.d.12, 1.d.13, 1.d.14, 1.d.15, 1.d.16, 1.d.17, 1.d.18, 1.d.19, 1.d.20, 1.d.21, 1.d.22, 1.d.23, 1.d.24, 1.d.25, 1.d.26, 1.d.27, 1.d.28, 1.d.29, 1.d.30, 1.d.31, 1.d.32, 1.d.33, 1.d.34, 1.d.35, 1.d.36, 1.d.37, 1.d.38, 1.d.39, 1.d.40, 1.d.41, 1.d.42, 1.d.43, 1.d.44, 1.d.45, 1.d.46, 1.d.47, 1.d.48, 1.d.49, 1.d.50, 1.d.51, 1.d.52, 1.d.53, 1.d.54, 1.d.55, 1.d.56, 1.d.57, 1.d.58, 1.d.59, 1.d.60, 1.d.61, 1.d.62, 1.d.63, 1.d.64, 1.d.65, 1.d.66, 1.d.67, 1.d.68, 1.d.69, 1.d.70, 1.d.71, 1.d.72, 1.d.73, 1.d.74, 1.d.75, 1.d.76, 1.d.77, 1.d.78, 1.d.79, 1.d.80, 1.d.81, 1.d.82, 1.d.83, 1.d.84, 1.d.85, 1.d.86, 1.d.87, 1.d.88, 1.d.89, 1.d.90, 1.d.91, 1.d.92, 1.d.93, 1.d.94, 1.d.95, 1.d.96, 1.d.97, 1.d.98, 1.d.99, 1.d.100

احم أسرارك المفردات



الخصوصية: حماية البيانات والمعلومات الشخصية (وتدعى أيضًا بالمعلومات الحساسة)

الأمان: حماية الأجهزة والبرامج الموجودة عليها

التحقق بخطوتين (يُعرف أيضًا بالتحقق أو المصادقة الثنائية): وهو وسيلة أمنية تتطلب خطوتين أو عاملين منفصلين، مثل كلمة مرور ورمز لمرة واحدة، من أجل تسجيل الدخول إلى إحدى الخدمات. على سبيل المثال، قد يُطلب منك إدخال كلمة المرور الخاصة بك ومن ثم إدخال رمز تم إرساله إلى هاتفك أو رمز من التطبيق.

كلمة المرور أو رمز المرور: كلمة سرية تستخدم للدخول إلى إحدى الخدمات. وقد تتخذ أشكالاً مختلفة، على سبيل المثال، قد يكون لديك رمز مكون من أربعة أرقام فقط تستخدمه لقفل هاتفك وكلمة مرور أكثر تعقيداً لحساب البريد الإلكتروني الخاص بك. بشكل عام، يجب أن تنشئ كلمات مرور طويلة ومعقدة قدر الإمكان وتستطيع مع ذلك تذكرها.

التشفير: عملية تحويل المعلومات أو البيانات إلى رموز تجعلها غير قابلة للقراءة ولا يمكن الوصول إليها

التعقيد: وهو المطلوب عند إنشاء كلمة مرور آمنة. على سبيل المثال، تحتوي كلمة مرور معقدة على مجموعة من الأرقام والأحرف الخاصة (مثل "\$" أو "&") والأحرف الصغيرة والكبيرة.

مُخترق: شخص يستخدم أجهزة الكمبيوتر للوصول غير المصرح به إلى أجهزة وبيانات تابعة للآخرين أو للمؤسسات

احم أسرارك: النشاط 1

كيف تختار كلمة مرور قوية

يتعلم الطلاب كيفية إنشاء كلمة مرور قوية والحفاظ على سرّيتها بعد إنشائها.

الأهداف بالنسبة للطلاب



- ✓ **التعرّف على** أهمية عدم مشاركة كلمات المرور مطلقًا، باستثناء مع الأهل أو الأوصياء
- ✓ **إدراك** أهمية قفل الشاشة لحماية الأجهزة
- ✓ **معرفة** كيفية إنشاء كلمات مرور يصعب تخمينها بها، ولكن يسهل تذكرها
- ✓ **اختيار** إعدادات الأمان المناسبة عند تسجيل الدخول، بما في ذلك التحقق بخطوتين

دعونا نتحدث



السلامة خير من الندامة

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 مع أصدقائك؟)

لكن نفس الأدوات التي تسهّل علينا تبادل المعلومات تسهّل أيضًا على المُخترقين والمحتالين سرقة تلك المعلومات واستخدامها لإلحاق الضرر بأجهزتنا وعلاقاتنا وسمعتنا.

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

• من يستطيع أن يخمن كلمات السر الأكثر استخدامًا؟

(الجواب: "1 2 3 4 5 6" و "password")

• دعونا نتحدث عن بعض كلمات المرور غير المناسبة الأخرى وما يجعلها غير مناسبة. (أمثلة: اسمك الكامل ورقم هاتفك وكلمة "chocolate")

من يعتقد أن كلمات المرور هذه جيدة؟

النشاط



المواد المطلوبة:

- أجهزة متصلة بالإنترنت للطلاب أو مجموعات الطلاب
- لوح معلومات أو شاشة عرض
- مستند "دليل إنشاء كلمات المرور القوية" يتم توزيعه على الطلاب

إليك فكرة لإنشاء كلمة مرور آمنة للغاية:

- فكّر في عبارة مضحكة يمكنك تذكّرها. قد تكون أغنيتك المفضلة أو عنوان كتاب أو عبارة مميزة من فيلم، إلخ.
- اختر أول حرف أو حرفين من كل كلمة في العبارة.
- غيّر بعض الحروف إلى رموز أو أرقام.
- اجعل بعض الحروف كبيرة وبعض الحروف الصغيرة.
- لتتضمن على مهارتنا الجديدة من خلال لعبة كلمة المرور.

1. إنشاء كلمات مرور

لنتوزع في فرق مكوّنة من فردين. لدى كل فريق 60 ثانية لإنشاء كلمة مرور. (اقترح لتحدي: يشارك الطلاب الأدلة مع الصف أو لأ لمعرفة مقدار المعلومات السياقية التي يحتاجها الطلاب لتخمين كلمات المرور بدقة.)

2. مقارنة كلمات المرور

سيقوم فريقان في كل مرة بالتزامن بكتابة كلمة المرور الخاصة بهما على اللوح.

التكملة في الصفحة التالية ←

3. تصويت

يتم التصويت على كل زوج من كلمات المرور ومناقشة أيها أقوى.

الخلاصة

دليل إنشاء كلمات المرور القوية

من المهم والممتع لإنشاء كلمات مرور قوية.

إليك بعض النصائح لإنشاء كلمات مرور للحفاظ على أمان معلوماتك.

كلمات المرور القوية هي عبارة أو جملة وصفية يسهل عليك تذكرها ويصعب على الآخرين تخمينها، مثل الأحرف الأولى في الكلمات في عنوان كتاب أو أغنيتك المفضلة أو الأحرف الأولى للكلمات في جملة حول أمر ما قمت به، وتتضمن مزيجًا من الأحرف والأرقام والرموز. على سبيل المثال، يمكن استخدام "درست الصف الثالث في مدرسة وسترن الابتدائية" "I went to Western Elementary School for grade 3" لإنشاء كلمة مرور مثل: lw2We\$t4g3.

كلمات المرور المعتدلة هي كلمات مرور قوية لا يسهل على البرامج الضارة تخمينها، ولكن يمكن لمن يعرفونك تخمينها (على سبيل المثال، lwenttoWestern).

كلمات المرور الضعيفة تشمل عادةً معلومات شخصية مثل اسم الحيوان الأليف، ويمكن تخمينها بسهولة من قبل من يعرفونك (على سبيل المثال، "IloveBuddy" أو "Ilikechocolate").

خطوات ينبغي اتباعها

- استخدم كلمة مرور مختلفة لكل واحد من حساباتك المهمة.
- استخدم ثمانية أحرف على الأقل. كلما كانت كلمة المرور أطول كانت أقوى (طالما يمكنك تذكرها!).
- استخدم مزيجًا من الأحرف (الكبيرة والصغيرة) والأرقام والرموز.
- اختر كلمات مرور يسهل تذكرها حتى لا تحتاج إلى تدوينها والمخاطرة بكشفها.
- غيّر كلمة المرور على الفور إذا كنت تعرف أو تعتقد بأن شخصًا آخر غير موثوق به اكتشفها.
- استخدم دومًا أفعال شاشة قوية على أجهزتك. اضبط أجهزتك على القفل التلقائي تحسبًا لوقوعها في يد الأشخاص الخاطئ.
- فكر في استخدام مدير كلمات المرور، وقد يكون مضمّنًا في متصفحك، لتذكر كلمات المرور الخاصة بك. ويمكنك بهذه الطريقة استخدام كلمة مرور فريدة لكل حساب من حساباتك وليس عليك تذكرها جميعًا.

خطوات ينبغي تجنبها

- استخدام المعلومات الشخصية (مثل الاسم أو العنوان أو البريد الإلكتروني أو رقم الهاتف أو رقم الضمان الاجتماعي أو اسم الأم قبل الزواج أو تواريخ الميلاد، إلخ) أو الكلمات الشائعة في كلمة المرور الخاصة بك.
- استخدام كلمة مرور يسهل تخمينها، مثل لقبك أو اسم مدرستك فقط أو فريق كرة القدم المفضّل لديك أو سلسلة سهلة من الأرقام (مثل 123456)، إلخ. والابتعاد تمامًا عن استخدام كلمة "Password".
- مشاركة كلمة المرور مع أي شخص غير الأهل أو الوصي عليك.
- كتابة كلمات المرور حيث يمكن لأي شخص العثور عليها.

احم أسرارك: النشاط 2

كيف تحتفظ بها لنفسك

يستخدم المعلم جهازًا تابعًا للمدرسة لتوضيح وسائل تخصيص إعدادات الخصوصية وكيفية الوصول إليها.

الأهداف بالنسبة للطلاب

- ✓ تخصيص إعدادات الخصوصية للخدمات التي يستخدمونها على الإنترنت
- ✓ اتخاذ القرارات بشأن المعلومات التي تتم مشاركتها على المواقع والخدمات المستخدمة
- ✓ فهم الهدف من التحقق بخطوتين والتحقق بعاملين ومتى يجب استخدامهما



دعونا نتحدث



الخصوصية تساوي الأمان

يرتبط الأمان والخصوصية على الإنترنت ببعضهما. وتوفّر معظم التطبيقات والبرامج طرقًا للتحكم في نوع المعلومات التي نشاركها وكيفية مشاركتها.

عندما تستخدم تطبيقًا أو موقعًا على الويب، ابحث عن خيارات مثل "حسابي" أو "الإعدادات". ستجد هناك إعدادات الخصوصية والأمان التي تتيح لك اختيار:

- المعلومات التي تظهر في ملفك الشخصي
- الأشخاص الذين يستطيعون رؤية مشاركاتك أو صورك أو فيديوهاتك أو أي محتوى آخر تشاركه

وبعد تعلّم استخدام إعدادات الخصوصية هذه والحرص على تحديثها بشكل مستمر، ستتمكّن من إدارة خصوصيتك وأمانك على الإنترنت. من المهم تذكر أهمية مشاركة الأهل أو الوصي عليك دائمًا في اتخاذ هذه القرارات.

النشاط



المواد المطلوبة:

- جهاز تابع للمدرسة متصل بشاشة عرض ويتضمن حسابًا يمكن استخدامه في الصف (مثل بريد إلكتروني مؤقت أو حساب على موقع إلكتروني)

خيارات العرض

تم ربط جهاز تابع للمدرسة بشاشة العرض. لننتقل إلى صفحة الإعدادات في هذا التطبيق حيث يمكننا أن نرى الخيارات المتوفرة. دُكروني بالخطوات (شجّع طلابك على مساعدتك في) ...

- تغيير كلمة المرور
- مراجعة إعدادات المشاركة والموقع الجغرافي والإعدادات الأخرى وتحديد أيها الأنسب
- تلقّي تنبيهات عند محاولة تسجيل الدخول إلى حسابك من جهاز غير معروف
- جعل ملفك الشخصي على الإنترنت، بما في ذلك الصور والفيديوهات، مرئيًا للعائلة والأصدقاء الذين تختارهم فقط
- تفعيل تدبير التحقق بعاملين أو بخطوتين
- إعداد معلومات استرداد الحساب في حال عدم التمكن من تسجيل الدخول إليه

عليك مناقشة إعدادات الخصوصية والأمان المناسبة لك مع أهلك أو الوصي عليك. ولكن تذكر بأن أهم إعدادات الأمان موجودة في ذهنك، حيث أنك أنت من يقرّر حجم المعلومات الشخصية التي تريد مشاركتها والتوقيت المناسب والأشخاص المناسبين.

الخلاصة

يعد اختيار كلمة مرور قوية وفريدة لكل حساب من حساباتك المهمة خطوة أولى رائعة. أما الخطوة الثانية فهي تذكر كلمات المرور الخاصة بك والاحتفاظ بها فقط لنفسك.

احم أسرارك: النشاط 3

"عالم الإنترنت": قلعة الأمان

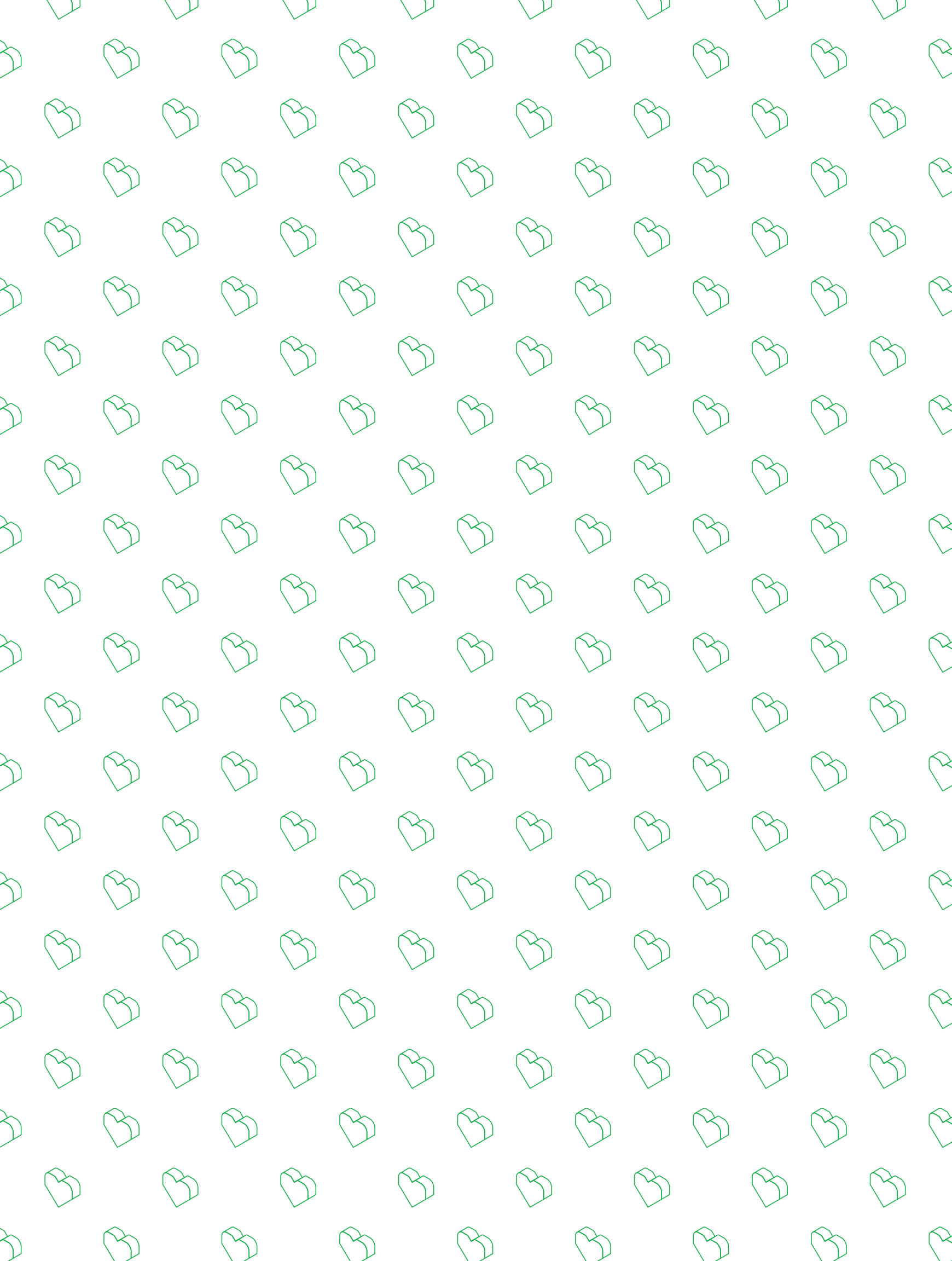
النجدة! لقد تم فتح قفل قلعة الأمان وأصبحت معلومات المستخدم القيمة مثل معلومات الاتصال والرسائل الخاصة معرضة لخطر كبير. تجنّب المُخترقين وشيّد قلعة باستخدام كلمات مرور قوية لحماية أسرارك إلى الأبد.

افتح متصفح ويب على جهاز الكمبيوتر أو جهاز جوّال (مثل الجهاز اللوحي)، وانتقل إلى [g.co/TowerOfTreasure](https://www.g.co/TowerOfTreasure)

مواضيع النقاش



- اطلب من طلابك لعب مرحلة "قلعة الأمان" واستخدم الأسئلة التالية لتشجيع المزيد من النقاش حول الدروس المستقاة من اللعبة. يستفيد معظم الطلاب إلى أقصى حدّ إذا لعبوا بشكل فردي، ولكن يمكن أيضًا تقسيم الطلاب إلى فرق من لاعبين. وقد يستفيد الطلاب الأصغر سنًا من ذلك بشكل خاص.
- ما العناصر التي تُؤلف كلمة مرور "فائقة القوة"؟
 - متى يكون من المهم إنشاء كلمات مرور قوية في الحياة الواقعية؟ ما هي النصائح التي تعلمتها حول كيفية القيام بذلك؟
 - من هو المُخترق؟ صف سلوك هذه الشخصية وتأثيرها على اللعبة.
 - هل أدى لعب مرحلة "قلعة الأمان" إلى تغيير طريقة تخطيطك لحماية معلوماتك في المستقبل؟
 - اذكر تصرّفًا مختلفًا ستلتزم به نتيجة ما تعلمته من هذه الدروس ومن اللعبة.
 - تمرّن على إنشاء ثلاث كلمات مرور "فائقة القوة".
 - أعط أمثلة على معلومات حساسة يجب حمايتها؟



اللطافة من سمات الأبطال

قوة الإيجابية على الإنترنت

نظرة عامة على الدرس

- النشاط 1: من متفرجين إلى مدافعين
- النشاط 2: خيارات المدافعين
- النشاط 3: ... ولكن قل ذلك بلطف!
- النشاط 4: انتبه لنبرتك
- النشاط 5: قبول التحدي
- النشاط 6: "عالم الإنترنت": مملكة اللطافة

المواضيع

يخلق العالم الرقمي تحديات وفرصًا جديدة للتفاعل الاجتماعي لجميع المستخدمين، قد يصعب قراءة الإشارات الاجتماعية على الإنترنت، وقد يسبب التواصل المستمر الراحة والقلق على حد سواء، كما يمكن أن يؤدي إخفاء الهوية إلى زيادة الإعجاب والمجاملات بالإضافة إلى إلحاق الأذى بالذات والآخرين.

هذا الأمر معقد بعض الشيء، ولكننا نعلم بأن الإنترنت قدرة على زيادة تأثير اللطافة أو السلبية على حد سواء. ومن الضروري تعلّم كيفية التعبير بلطف وبتعاطف وكيفية الاستجابة للسلبية والمضايقة من أجل بناء علاقات صحية والحد من مشاعر العزلة التي تؤدي في بعض الأحيان إلى التنمر والاكنتاب وصعوبات التعلّم وغيرها من المشاكل.

تُشير الأبحاث إلى أنه بدلاً من نهي الأطفال عن التصرف بسلبية على الإنترنت، يجب التحدث عن سبل الحدّ من التنمر لمعالجة الأسباب الكامنة وراء السلوك السلبي. وتشجّع هذه الأنشطة الطلاب على التفاعل بشكل إيجابي من البداية وتعلمهم كيفية التعامل مع السلبية عند ظهورها.

الأهداف بالنسبة للطلاب

- ✓ تعريف السلوك الإيجابي ومميزاته على الإنترنت وفي الواقع
- ✓ التعامل بإيجابية خلال التواصل على الإنترنت
- ✓ تحديد الحالات التي يجب الرجوع فيها إلى شخص بالغ موثوق به

المعايير ذات الصلة

- معايير ISTE للمعلمين: 1a, 1c, 2c, 3a, 3b, 3c, 4b, 5a, 5b, 6a, 6b, 6d, 7a
- معايير جامعة ISTE للطلاب لعام 2016: 1c, 2b, 3d, 4d, 7a, 7b, 7c
- معايير AASL التعليمية: I.c.1, I.c.2, I.c.3, I.d.3, I.d.4, II.a.1, II.a.2, II.b.1, II.b.2, II.b.3, II.c.1, II.c.2, II.c.3, II.d.1, II.d.2, II.d.3, III.a.1, III.a.2, III.a.3, III.b.1, III.b.2, III.c.1, III.c.2, III.d.1, III.d.2, IV.b.2, IV.b.3, IV.d.2, V.a.2, V.a.3, V.c.1, V.c.3, V.d.1, V.d.2, V.d.3, VI.a.1, VI.a.2, VI.d.1, VI.d.3

اللطافة من سمات الأبطال المفردات



التنمّر: هو سلوك مسيء مقصود ومتكرّر. وغالبًا ما يواجه الشخص المستهدف صعوبة في الدفاع عن نفسه

التنمّر على الإنترنت: التنمّر الذي يحدث على الإنترنت أو من خلال استخدام الأجهزة الرقمية

المضايقة: مصطلح أكثر عمومية من التنمّر ويمكن أن يتخذ أشكالاً عديدة، مثل المضايقة أو الإزعاج أو التخويف أو الإهانة أو غيرها، ويمكن أن يحدث على الإنترنت أيضًا

نزاع: صراع أو خلاف ليس من الضروري أن يكون متكرّرًا

المعتدي: الشخص الذي يقوم بالمضايقة أو التنمّر، والذي يُطلق عليه أحيانًا اسم "المتنمّر"، على الرغم من أن خبراء منع التنمّر ينصحون بعدم تصنيف الأشخاص على هذا النحو

الشخص المستهدف: الشخص الذي يتعرض للتخويف أو الأذى

المتفرج: شاهد على المضايقة أو التنمّر يدرك ما يجري ولكنه يختار عدم التدخل

المدافع: شاهد على المضايقة أو التنمّر يدعم الضحية سرًا أو علنًا، وقد يحاول أحيانًا إيقاف الحادث و/أو الإبلاغ عنه

زيادة الأثر: زيادة أو توسيع المشاركة أو التأثير

الإقصاء: شكل من أشكال المضايقة أو التنمّر على الإنترنت وفي الواقع؛ يشار إليه في كثير من الأحيان باسم "الإقصاء الاجتماعي"

الخطر: طريقة لإنهاء كل تواصل مع شخص آخر على الإنترنت ومنعه من الوصول إلى ملفك الشخصي ومراسلتك ورؤية مشاركاتك وما إلى ذلك، دون إعلامه بذلك (ليس دائمًا الحلّ المثالي في حالات التنمّر حين يريد الشخص المستهدف معرفة ما يقوله المعتدي أو إذا توقف التنمّر)

التجاهل: طريقة أقل حسماً للتوقف عن رؤية ما ينشره الشخص الآخر من مشاركات وتعليقات وما إلى ذلك في وسائل التواصل الاجتماعي، وذلك عندما يصبح التواصل معه مزعجًا. ويتم ذلك دون إبلاغ هذا الشخص ودون التوقف عن الظهور في الخلاصة لديهم (ليس حلًا مفيدًا في حالات التنمّر)

مجهول الهوية: شخص مجهول الهوية أو غير معروف - شخص على الإنترنت لا تعرف اسمه أو هويته

الاستفزاز: النشر أو التعليق على الإنترنت بطريقة قاسية أو عدوانية أو استفزازية

الإبلاغ عن إساءة الاستخدام: استخدام أدوات أو نظام في وسائل التواصل الاجتماعي للإبلاغ عن المضايقات والتنمّر والتهديدات وغيرها من المحتويات الضارة التي تخالف عادةً بنود الخدمة أو معايير المنتدى

اللطافة من سمات الأبطال: النشاط 1

من متفرجين إلى مدافعين

يتمرن الطلاب على تحديد الأدوار الأربعة في حالات التنمر (الشخص المتنمر، الشخص المستهدف بالتنمر، المتفرج، والمدافع) وما الذي يجب فعله إذا كانوا متفرجين أو مستهدفين بالتنمر.

الأهداف بالنسبة للطلاب

- ✓ التعرف على حالات المضايقة أو التنمر على الإنترنت
- ✓ مناقشة معنى أن تكون متفرجًا أو مدافعًا على الإنترنت
- ✓ تعلم طرق محددة للتعامل مع التنمر عند حدوثه
- ✓ معرفة كيفية التصرف عند التعرض للمضايقة



دعونا نتحدث



لماذا تعتبر اللطافة مهمة؟

- من المهم ان نتذكر دائماً أن وراء كل اسم مستخدم وكل صورة رمزية شخصًا حقيقيًا لديه مشاعر حقيقية، ويجب أن نعامله كما نتمنى لأنفسنا. عادةً ما يشارك في التنمر أو أي سلوك مسيء آخر أربعة أنواع من الأشخاص.
- هناك المعتدي، أو الشخص المتنمر.
 - هناك أيضًا الشخص الذي يتعرض للتنمر أو الشخص المستهدف.
 - هناك الشهود على الحدث، وغالبًا ما يُعرفون بالمتفرجين.
 - وهناك شهود على الحدث يحاولون التدخل بشكل إيجابي، وغالبًا ما يُعرفون بالمدافعين.

إذا تعرضت للتنمر أو أي سلوك مسيء آخر على الإنترنت، إليك بعض الأمور التي يمكنك القيام بها:

إذا كنت مستهدفًا، يمكنكني...

- عدم الرد
- حظر الشخص
- الإبلاغ عنه - إخبار أحد والدي أو معلمي أو أحد أصدقائي أو أي شخص آخر أثق به واستخدام أدوات الإبلاغ في التطبيق أو الخدمة للإبلاغ عن المشاركة أو التعليق أو الصورة المسيئة

إذا كنت شاهدًا على حدوث مضايقة أو تنمر، لديك خيار التدخل والإبلاغ عن السلوك المسيء. في بعض الأحيان لا يحاول المتفرجون إيقاف التنمر أو مساعدة الشخص المستهدف، ولكن عندما يفعلون ذلك فهم يتحولون إلى مدافعين. يمكنك الاختيار بأن تكون مدافعًا من خلال اتخاذ قرار بعدم دعم السلوك الفظ والدفاع عن اللطافة والإيجابية. وقد يكون للقليل من الإيجابية صدى كبير على الإنترنت. فهي قد تمنع انتشار السلبية وتحولها إلى سلوكيات قاسية ومؤذية.

بإمكاني التحول من متفرج إلى مدافع من خلال...

- العثور على طريقة لمواساة الشخص المستهدف أو دعمه
- انتقاد السلوك الفظ في تعليق أو رد (تذكر أن تنتقد السلوك وليس الشخص) إذا كنت تعتقد أن ذلك أنه لا يشكل خطرًا عليك
- اتخاذ قرار بعدم مساعدة المعتدي من خلال نشر التنمر أو زيادة الضرر من خلال مشاركة المنشور أو التعليق الفظ على الإنترنت
- إقناع مجموعة من الأصدقاء بإنشاء "مجموعة اللطف" ونشر الكثير من التعليقات اللطيفة عن الضحية (ولكن دون الإساءة للمعتدي، لأنكم تهدفون لإعطاء مثال وليس للانتقام)
- الإبلاغ عن المضايقة: إخبار أي شخص يمكنه المساعدة مثل أحد الوالدين أو المعلم أو مستشار المدرسة

النشاط



المواد المطلوبة:

- مستند ورقة عمل "من متفرجين إلى مدافعين" يتم توزيعه على الطلاب

إجابات ورقة عمل "من متفرجين إلى مدافعين"

السيناريو الأول: B, U, B (لأن ذلك لا يساعد على حل الموقف), U, U

السيناريو الثاني: U, B, U, U

السيناريو الثالث: U, U, B, B, U

السيناريو الرابع: أنتم تحددون الإجابات

1. قراءة السيناريوهات وتصنيف الردود

بعد مناقشة الأدوار، ورّع ورقة العمل على الطلاب وأعطهم 15 دقيقة لقراءة السيناريوهات الثلاثة وتصنيف كل رد. إذا تبقى ما يكفي من الوقت، اطلب من الطلاب وضع سيناريو رابع.

2. مناقشة الأجوبة

قبل المناقشة أو عند انتهائها، اسأل الطلاب عن إيجابيات وجود المدافعين في المدرسة أو على الإنترنت.

3. مناقشة الردود التي كان من الصعب تصنيفها

إذا تبقى ما يكفي من الوقت، اسأل طلابك إذا واجهوا صعوبة في تصنيف أي من الردود والسبب في ذلك. ناقشهم حول هذه المسألة.

الخلاصة

سواء دافعت عن الآخرين أو أبلغت عن إساءة أو تجاهلت أمرًا ما بهدف عدم زيادة أثره، لديك مجموعة متنوعة من الحلول التي تناسب كل موقف. وبقليل من اللطافة، يمكن لأي شخص إحداث فرق كبير وقلب المواقف السلبية إلى إيجابية.

ورقة عمل: النشاط 1

من متفرجين إلى مدافعين

أصبحت تعرف الآن بأنه يمكن للمتفرج اتخاذ قرار بفعل الصواب وأن يتحول إلى مدافع من خلال مساعدة الشخص الذي يتعرض للتنمر. سنرى في ما يلي ثلاثة سيناريوهات تمثل حالات تنمر أو مضايقة على الإنترنت، كما يمكننا تأليف سيناريو رابع حدث مع أشخاص تعرفهم واقتراح ردود قد تصدر عن المتفرجين والمدافعين. يحتوي كل من السيناريوهات الثلاثة التي تم وضعها على مجموعة ردود. اقرأ كلاً منها وقرر ما إذا كان صادراً عن متفرج أو مدافع، ثم ضع حرف "B" للإشارة إلى المتفرج وحرف "U" للإشارة إلى المدافع في الفراغ بجانب الرد. إذا تبقى ما يكفي من الوقت ناقش في الصف الردود التي كان من الصعب تصنيفها وأسباب ذلك.

السيناريو الأول

أوقعت إحدى صديقاتك هاتفها بجانب نافورة مياه الشرب بالقرب من ملعب كرة القدم في المدرسة. وجد شخص الهاتف واستخدمه لإرسال رسالة فظة للغاية عن طالب آخر إلى مجموعة من أفراد فريق كرة القدم، ثم أعاد الهاتف إلى حيث وجده. ويقول الشخص المستهدف لصديقتك إنها شخص فظيع بسبب إرسالها لتلك الرسالة، على الرغم من أنها ليست من أرسلها. ولا أحد يعرف من الذي أرسل الرسالة الفظة. فهل...

تشعر بالحزن لما حدث لصديقتك ولكنك لن تفعل شيئاً لأن لا أحد يعرف من سبب لها هذا.

تعثر على الشخص المستهدف وتواسيه وتساءله إذا كان بإمكانك مساعدته.

تنشر الحدث من خلال مشاركة الرسالة الفظة مع الأصدقاء الآخرين.

تطلب أنت وصديقتك من الجميع في فريق كرة القدم نشر أمور إيجابية عن الشخص المستهدف.

تبلغ أنت وصديقتك المدير عن الحادث بشكل سري، وتشير إلى ضرورة توعية الجميع حول أهمية تأمين الهواتف وقفلها.

السيناريو الثاني

أنشأت معلمتك مدونة للصف في موضوع فنون اللغة لإعطاء الطلاب مساحة للكتابة والتحرير ونشر التعليقات. في اليوم التالي تغيبت المعلمة عن المدرسة بسبب المرض ولم يلاحظ المعلم البديل بأن الأمور ليست على ما يرام في مدونة الصف حيث قام أحد الطلاب بكتابة تعليقات فظة عن طالب آخر في الصف. فهل...

ترد على التعليقات بأمر مثل "هذا ليس مضحكاً" أو "أنا صديق _____، وهذا ليس صحيحاً".

تتجاهل الموضوع حتى عودة المعلمة.

تطلب من الطلاب الآخرين كتابة تعليقات وأمور إيجابية عن الطالب المستهدف.

تخبر المعلم البديل حول ما يحدث في مدونة الصف وقد يقرر إبلاغ المعلمة بذلك.

السيناريو الثالث

هناك لعبة على الإنترنت يلعبها مجموعة من أصدقائك كثيرًا. عادة ما تكون الدردشة في اللعبة حول ما يحدث في اللعبة نفسها. في بعض الأحيان يحتدم النقاش قليلاً، إلا أن ذلك يكون عادة أقرب إلى التنافس الودي منه إلى الإساءة. ولكن هذه المرة بدأ أحد اللاعبين بقول أمور سيئة للغاية عن أحد أصدقائك المشاركين في اللعبة، واستمر في ذلك. كما أنه واصل ذلك في اليوم التالي. فهل...

□ تتصل بصديقك وتخبره بأنك مستاء بقدره مما يحدث وتناقش معه ما يجب القيام به.

□ تتصل بجميع اللاعبين الذين تعرفهم (بعلم صديقك) لمعرفة ما إذا كانوا جميعاً متفقين على الاعتراض على هذا التصرف الفظ.

□ تقرر الانتظار لترى ما إذا كان هذا التصرف سيتوقف، ثم ربما تتصرف حيال الأمر.

□ تبتعد عن اللعبة لبعض الوقت.

□ تبحث عن قواعد منتدى اللعبة وتقوم بالإبلاغ عن التنمر إذا كان منافياً لهذه القواعد باستخدام نظام الإبلاغ في اللعبة.

السيناريو الرابع

اطلب من الطلاب أن يتعاونوا على تأليف سيناريو من الحياة الواقعية، استناداً إلى موقف سمع عنه أحدهم، ومن ثم ابتكار ردود لمدافعين ومفرجين لإثبات فهمهم لمحتويات هذا القسم.

اللطافة من سمات الأبطال: النشاط 2

خيارات المدافعين

يرغب الطلاب غالبًا في مساعدة الشخص المستهدف بالتئمّر ولكنهم لا يعرفون ما يمكنهم فعله. يوضح هذا النشاط الخيارات القائمة ويقدم أمثلة لمساعدتهم على اقتراح ردود إيجابية بنفسهم.

الأهداف بالنسبة للطلاب

- ✓ الإدراك بأن لعب دور المدافع هو خيار
- ✓ تعلّم الطرق المختلفة للتدخّل ولعب دور المدافع في مواقف معيّنة
- ✓ اختيار طريقة الرد الأنسب والأكثر أمانًا
- ✓ اقتراح رد خاص على الموقف.



دعونا نتحدث



عندما تشهد شخصًا يسخر من شخص آخر على الإنترنت أو يقلل من احترامه أو يؤذي مشاعره أو يتصرّف معه بطريقة تسبب له الإحراج أو تشعره بالإقصاء، تدكّر بأن لديك خيارات يمكنك أن تتصرف وفقها. أولًا، يمكنك اختيار أن تكون مدافعًا بدلًا من متفرج من خلال مساعدة الشخص المستهدف. ثانيًا، إذا اخترت أن تكون مدافعًا، لديك العديد من الخيارات حول طرق التعامل الممكنة.

أهم ما يجب معرفته هو أنه بالإمكان مساعدة الشخص المستهدف بمجرد مواساته وجعله يشعر بأن هناك من يهتم لأمره.

قد لا يشعر الجميع بالراحة في مواجهة الآخرين علنًا سواء على الإنترنت أو في غرفة الطعام في المدرسة. إذا كنت مستعدًا لذلك، لا تتردد! بإمكانك...

- انتقاد السلوك الفظ (وليس الشخص)، ووصفه بأنه غير لطيف
- قول أمر لطيف 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 في الملعب أو الانضمام إليك وقت الغداء

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 (إذا كنت تستخدم وسائل تتيح لك البقاء مجهول الهوية)
- إخباره بأنك مستعد للإصغاء إذا رغب في التحدث بعد المدرسة
- خلال محادثة هادئة شخصيًا أو على الهاتف، يمكنك إخباره بأنك تعتقد بأن السلوك المسيء كان خاطئًا وأسأله إذا كان يرغب بالحديث عما حدث

بغض النظر عن الطريقة التي تختارها لتكون مدافعًا، تتوفر لك خيارات علنية وغير علنية للإبلاغ عن التئمّر. مثل الإبلاغ عبر موقع الويب أو واجهة التطبيق، أو الإبلاغ عن الحدث لشخص بالغ تثق به.

النشاط



المواد المطلوبة:

- لوح أبيض أو حامل يلصق الطلاب عليه أوراق الملاحظات اللاصقة
- مستند ورقة عمل "خيارات المدافعين" يتم توزيعه على الطلاب
- أوراق ملاحظات لاصقة لكل مجموعة

سنلعب في هذا النشاط دور المدافعين، ولذلك لنفترض أن الصف بأكمله اختار مساعدة الشخص المستهدف.

1. يتوزع الطلاب في مجموعات مؤلفة من خمسة طلاب

على كل مجموعة تحديد قارئ وكاتب.

2. تقرأ المجموعات المواقف المؤذية وتناقشها معاً

تفاصيل المواقف الثلاثة مذكورة في ورقة العمل في الصفحة التالية.

خلال المناقشة في المجموعات، يقوم المعلم بقسم اللوح إلى مساحتين كبيرتين تحملان العنوانين "الدعم العلني" و "الدعم الخاص".

3. تختار المجموعات أو تقترح نوعين من الردود لكل منها

يستطيع الطلاب استخدام أمثلة الردود في "دعونا نتحدث" أو اقتراح ردود أخرى.

4. يشارك الطلاب اختياراتهم على اللوح ويقرؤونها بصوت عالٍ أمام الصف

يمكن للمعلم بعد ذلك توجيه المناقشة في الصف استناداً إلى اختيارات الطلاب.

الخلاصة

في كثير من الأحيان عندما ترى شخصاً يتعرض للأذى أو المضايقة، تريد مساعدته ولكنك لا تعرف دائماً ما يجب فعله. أصبحت الآن تعرف العديد من الطرق لمساعدة الشخص المستهدف وأنت تدرك بأنه لديك خيارات لتقديم الدعم له بالطريقة المريحة لك. لديك القدرة على مساعدة الآخرين بالطريقة التي تناسبك.

ورقة عمل: النشاط 2

خيارات المدافعين

بعد التوزع في مجموعات، تقرر كل مجموعة كيف يكون دور الشخص المدافع. اطلب من أحد المتطوعين في مجموعتك أن يسجل الردود (على أوراق الملاحظات اللاصقة) ومن متطوع آخر أن يقوم بالقراءة. يقرأ القارئ الموقف الأول بصوت عالٍ، ومن ثم تناقش المجموعات كل موقف لمدة خمس دقائق وتقرر كيف يمكن دعم الشخص المستهدف بشكل علني وبشكل خاص. يسجل الكاتب قرارات المجموعة على أوراق الملاحظات اللاصقة ويلصق إحداها في عمود "المساعدة بشكل علني" وأخرى في عمود "المساعدة بشكل خاص" على اللوح. لاتخاذ قرار، استخدم الأفكار التي ناقشها الطلاب معاً أو اقترح طريقتك الخاصة لمساعدة الشخص المستهدف. كرر هذه العملية للموقف الثاني والثالث.

ملاحظة: لا توجد طريقة واحدة صحيحة لدعم الشخص المستهدف لأن كل شخص (سواء كان مستهدفاً أو متفرجاً) يختلف عن الآخر كما يختلف كل موقف عن الآخر. نحن نحاول فقط تجربة أدوات مختلفة للمدافعين.

الموقف الأول

ينشر أحد الطلاب فيديو له وهو يغني أغنية لفنان بوب مشهور. يبدأ طلاب آخرون بنشر تعليقات فظة أسفل الفيديو. ما الذي يمكنك فعله لدعم الطالب الذي نشر الفيديو؟ استخدم بعض الأفكار التي ناقشناها سابقاً أو اتفق مع مجموعتك على رد جديد.

الموقف الثاني

يرسل أحد الطلاب لزميله لقطة شاشة عن تعليق نشره صديقك ويطلق مزحة فظة عنه. وتم إعادة نشر لقطة الشاشة وانتشرت بسرعة بين الطلاب في المدرسة. ما الذي يمكنك فعله لدعم الطالب الذي تم نشر تعليقه؟ اختر إحدى الأفكار التي تمت مناقشتها للتو في الصف، أو اقترح ردك الخاص.

الموقف الثالث

اكتشفت بأن طالباً في مدرستك أنشأ حساب تواصل اجتماعي مزيفاً مستخدماً اسم طالب آخر ونشر صوراً ومشاركات مضحكة تسخر من طلاب آخرين ومن المعلمين والمدرسة. ماذا تفعل لدعم الطالب الذي تم انتحال هويته بهذه الطريقة؟ فكر في بعض الحلول التي تمت مناقشتها سابقاً أو اقترح حلاً خاصاً بك.

اللطافة من سمات الأبطال: النشاط 3 ...ولكن قل ذلك بلطف!

في هذا النشاط، يعمل الطلاب معًا لإعادة صياغة التعليقات السلبية من أجل معرفة كيفية تحويل التفاعلات السلبية إلى تفاعلات إيجابية.

الأهداف بالنسبة للطلاب

- ✓ التعبير عن المشاعر والآراء بطرق إيجابية وفعالة
- ✓ الرد على السلبية بطرق بناءة وحضارية



دعونا نتحدث



تحويل السلبية إلى إيجابية

- يتعرض الأولاد في سنك لجميع أنواع المحتويات على الإنترنت، وبعضها يتضمن رسائل سلبية ترُوج لسلوك مسيء.
- هل صادفت (أنت أو أحد معارفك) شخصًا يتصرف بسلبية على الإنترنت؟ ماذا كان شعورك تجاه ذلك؟
 - هل سبق لك (أنت أو أحد معارفك) اختبار لفتة لطيفة عشوائية على الإنترنت؟ ماذا كان شعورك تجاه ذلك؟
 - ما هي الإجراءات البسيطة التي يمكننا اتخاذها لتحويل التفاعلات السلبية إلى تفاعلات إيجابية؟

يمكننا الرد على المشاعر السلبية بطرق بناءة من خلال إعادة صياغة التعليقات غير الودية والتنبيه لنبيرتنا خلال التواصل على الإنترنت.

النشاط



المواد المطلوبة:

- لوح معلومات أو شاشة عرض
- مستند ورقة عمل "....ولكن قل ذلك بلطف!" يتم توزيعه على الطلاب
- أوراق ملاحظات لاصقة أو أجهزة للطلاب

1. قراءة التعليقات

نحن ننظر جميعًا إلى التعليقات السلبية.

2. مراجعة التعليقات

- لنتوزع الآن في مجموعات مؤلفة من ثلاثة طلاب ونقترح نوعين من الردود على هذه التعليقات:
- كيف يمكن التعبير عن هذه الآراء أو مايمثلها بطرق إيجابية وبناءة أكثر؟
 - إذا نشر أحد زملائك تعليقات مشابهة، كيف يمكنك الرد عليه بطريقة تجعل المحادثة أكثر إيجابية؟

ملاحظة للمعلم

قد يحتاج الطلاب الأصغر سنًا إلى بعض الأمثلة حول كيفية مراجعة التعليقات. قد يكون العمل معًا على حل مثال واحد في الصف وسيلة لضمان نجاح الطلاب عند التفكير بشكل مستقل.

3. عرض الردود

الآن ستعرض كل مجموعة ردودها في كلتا الحالتين.

الخلاصة

قد يؤدي الرد على أمر سلبي بشكلٍ إيجابي إلى جعل المحادثة أكثر متعة وتشويقًا، وهذا أفضل بكثير من إصلاح عواقب التعليق غير اللطيف.

ورقة عمل: النشاط 3

...ولكن قل ذلك بلطف!

اقرأ التعليقات أدناه. ثم ناقش الأسئلة التالية:

1. كيف يمكنك التعبير عن هذه الآراء أو ما يماثلها بطرق إيجابية وبناءة أكثر؟
2. إذا نشر أحد زملائك تعليقات مشابهة، كيف يمكنك الرد عليه بطريقة تجعل المحادثة أكثر إيجابية؟

استخدم الفراغ الموجود تحت كل تعليق لتسجيل الأفكار.

سيرتدي الجميع اللون الأحمر غدًا، ولكن لا تخبروا ليلي.

المضحك هو أن أدهم هو الوحيد في الصف الذي لن يشارك في الرحلة المدرسية هذا الأسبوع.

لا أقصد الإهانة، ولكن خط يدك بشع، من الأفضل أن تنضم إلى مجموعة أخرى في هذا المشروع.

آسف، أنا لا أعتقد أنه بإمكانك حضور حفلتي. فهي للأغنياء فقط.

يمكنك الانضمام إلى مجموعتنا فقط إذا أعطيتني معلومات تسجيل الدخول إلى حسابك.

أذناي تؤلماني، من قال لها أنها تستطيع الغناء؟



ألا تعتقدون أن "منى" تشبه السنافر؟

يفسر الطلاب المشاعر التي تنقلها الرسائل بهدف التمرّن على ممارسة التفكير النقدي وتجنّب سوء التفسير والنزاعات خلال التواصل على الإنترنت.

- ✓ اتخاذ القرارات الصحيحة في ما يتعلّق بما يمكن قوله وكيفية قوله وما إذا كان من الأفضل عدم قول أي شيء
- ✓ تحديد المواقف التي يُفضّل فيها الانتظار للتواصل وجهاً لوجه مع أحد الزملاء بدلاً من مراسلته على الفور

الأهداف بالنسبة للطلاب



دعونا نتحدث



من السهل إساءة الفهم

يستخدم الشباب أنواعًا مختلفة من التواصل في أنواع مختلفة من التفاعل، لكن الرسائل التي يتم إرسالها عبر الدردشة يمكن تفسيرها بشكل مختلف عن التواصل الشخصي المباشر أو عبر الهاتف.

هل سبق أن أسّيء فهم رسالة نصية أرسلتها؟ على سبيل المثال، هل سبق لك أن كتبت مزحة وأخذها صديقك على محمل الجد أو اعتقد أنها فظة؟

هل سبق لك أن أسأت فهم شخص آخر في رسالة نصية أو خلال الدردشة؟ ما الذي فعلته للمساعدة في توضيح المعنى؟ ما الذي كان بإمكانك فعله بشكل مختلف؟

1. مراجعة الرسائل

دعونا نلقي نظرة على أمثلة الرسائل المسجّلة على اللوح. قد يكون لدى طلاب الصف أمثلة جيدة أيضًا، لنقم بكتابتها على اللوح لمناقشتها.

- "هذا في غاية الروعة!"
- "لا يهم"
- "أنا غاضب جدًا منك"
- "اتصل بي الآن!"
- "حسنًا، لا بأس"

2. قراءة الرسائل بصوت عالٍ

اطلب من شخص واحد قراءة واحدة من الرسائل بصوت عالٍ بنبرة صوت معينة (على سبيل المثال 😊 😐 😞)

ما الذي تلاحظه؟ كيف يمكن للاخريين تفسيرها؟ كيف يمكن لكل "جهة مرسله" أن توصل قصدها بشكل أفضل؟

النشاط



المواد المطلوبة:

- أمثلة عن رسائل نصية تعرض على اللوح أو على جهاز العرض

الخلاصة

قد يصعب فهم مشاعر الشخص من خلال قراءة رسالته النصية. احرص على اختيار وسيلة التواصل المناسبة وعدم إعطاء الكثير من الأهمية لما يقوله لك الأشخاص على الإنترنت. إذا لم تكن واثقًا مما يعنيه الشخص الآخر، استفسر عن قصده من خلال التحدث معه شخصيًا أو عبر الهاتف.

اللطافة من سمات الأبطال: النشاط 5

قبول التحدي

يناقش الطلاب كيف يمكن للأطفال أن يكونوا قدوةً للبالغين أيضًا.

- ✓ التفكير في سلوك البالغين على الإنترنت
- ✓ التفكير كيف يمكن لتصرفات البالغين أن تقدم نموذجًا تحتذي به الأجيال الشابة

الأهداف بالنسبة للطلاب



دعونا نتحدث



ما الذي يمكن للأطفال تعلّمه من البالغين وما الذي يمكن للبالغين تعلّمه من الأطفال؟

من المهم تعليم اللطافة. ولكن من المهم أن نمارس اللطافة التي نعلمها. هناك الكثير من الأمثلة التي تبين أن ظاهرة التنمر والمضايقة لا تقتصر على الأطفال. يمكن النظر إلى كيفية تعامل البالغين أحيانًا مع بعضهم على الإنترنت، أو في وسائل الإعلام، أو في الازدحامات المرورية.

لقد تحدثنا عن مدى أهمية معاملة زملائك وأصدقائك بلطف على الإنترنت وفي الواقع. هل سبق أن رأيت بالغين يعاملون بعضهم بفظاظة؟ هل رأيت بالغين يتنمرون على بعضهم؟ (لنتذكر بأنه لا حاجة لذكر أسماء، لنتطرق فقط إلى السلوك).

هل تعتقد بأن جيلك قادر على بناء شبكة إنترنت أكثر لطفاً وإيجابية من تلك التي أنشأها بعض البالغين لأنفسهم؟ (يعتقد الكثير من البالغين بأنكم ستنجحون بشكل أفضل في هذا.)

هل تعتقد أن بعض الأطفال يبدأون بالتنمر أو التعليق بشكلٍ غير لائق لأنهم يرون البالغين من حولهم أو في الأخبار يقومون بذلك؟ جوابك هو نعم بالنسبة لكل ما سبق؟ يرجى إعطاء أمثلة. ما الذي يمكنك فعله بدلاً من ذلك - كيف يمكنك أن تكون قدوة أفضل للبالغين؟

ملاحظة للمعلم

فكر في نقل هذه المناقشة إلى المستوى التالي من خلال إطلاق "حملة اللطافة" في مدرستك، حيث يكتب كل طالب في بداية الحصّة رسالة إيجابية ويقدمها لطالب آخر، ما يخلق جوًّا من الإيجابية في الحصّة ويذكّر الطلاب بالقدرة الكبيرة لديهم على نشر الإيجابية على الإنترنت وخارجها. يمكنك بدء إحدى الحصص بهذا الشكل كل أسبوع

الخلاصة

سيكون للطريقة التي تتعامل بها أنت وأصدقاؤك على الإنترنت تأثيرًا كبيرًا على العالم الرقمي الذي يبينه جيلك، بالإضافة إلى العالم الفعلي.

اللطافة من سمات الأبطال: النشاط 6

"عالم الإنترنت": مملكة اللطافة

تنتقل المشاعر بين الأشخاص سواء كانت جيدة أو سلبية. وينشر المعتدون المشاعر السلبية في كل مكان، حتى في أجمل أقسام المدينة. احظر المعتدين وأبلغ عنهم لإيقاف سيطرتهم وعامل باقي المستخدمين بلطف لاستعادة الطبيعة المسالمة لهذا العالم.

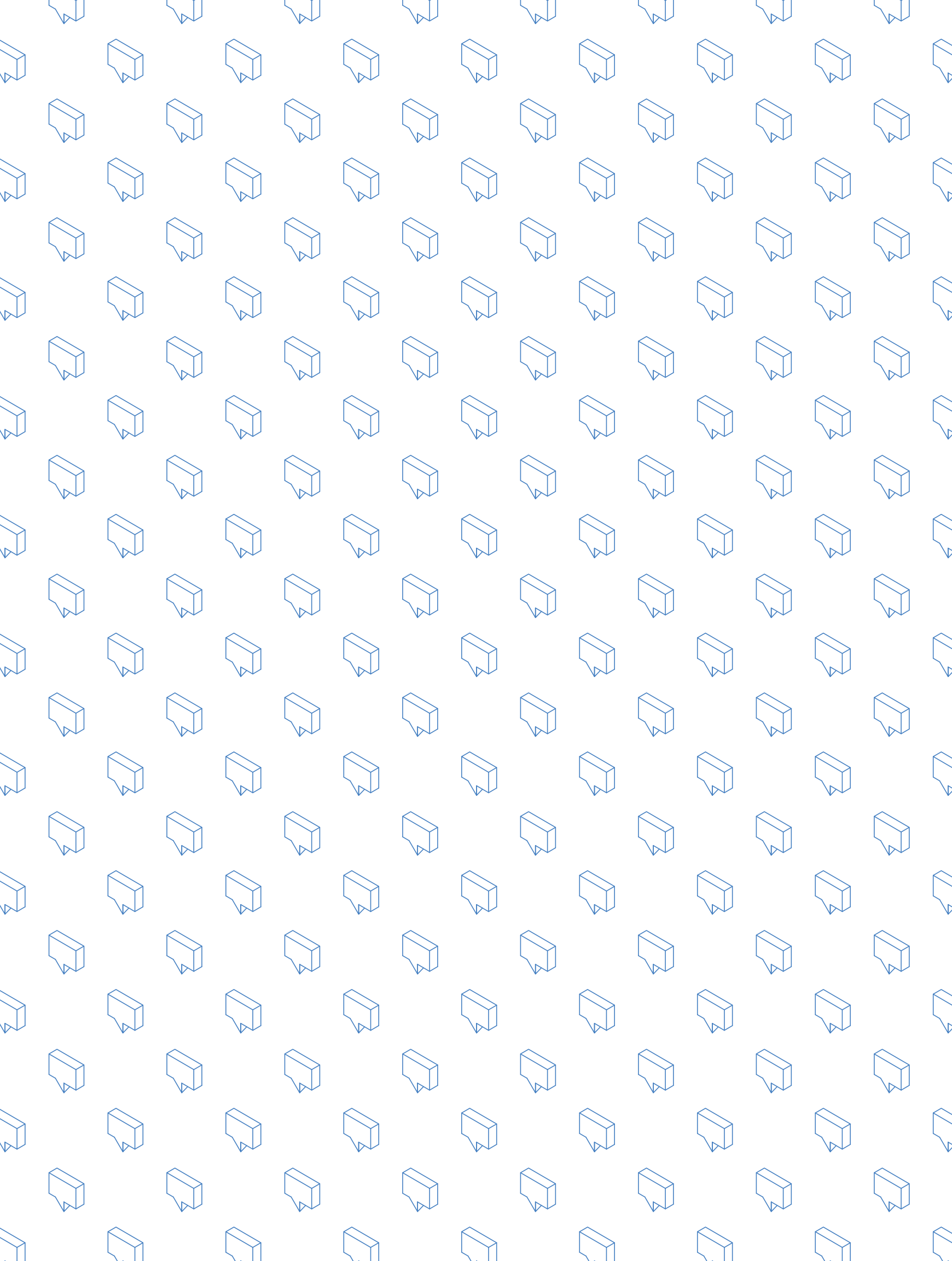
افتح متصفح ويب على جهاز الكمبيوتر أو جهاز جوال (مثل الجهاز اللوحي)، وانتقل إلى g.co/KindKingdom

مواضيع النقاش



- اطلب من طلابك لعب مرحلة "مملكة اللطافة" واستخدم الأسئلة التالية لتشجيع المزيد من النقاش حول الدروس المستفادة من اللعبة. يستفيد معظم الطلاب إلى أقصى حدّ إذا لعبوا بشكل فردي، ولكن يمكن أيضاً تقسيم الطلاب إلى فرق من لاعبين. وقد يستفيد الطلاب الأصغر سناً من ذلك بشكل خاص.
- ما هو السيناريو الأقرب لك في "مملكة اللطافة" ولماذا؟
 - أعط مثالاً على مرة ساهمت فيها بنشر اللطافة للآخرين على الإنترنت.
 - في أي حالات يكون من المناسب حظر شخص على الإنترنت؟
 - في أي حالات يكون من المناسب الإبلاغ عن سلوك شخص؟
 - برأيك، لماذا تُسمى الشخصية في "مملكة اللطافة" بـ "المعتدي"؟ صف سمات هذه الشخصية وكيف تؤثر أفعالها على اللعبة.
 - هل غيّر لعب "مملكة اللطافة" الطريقة التي تنوي التصرف بها مع الآخرين؟ إذا كان الجواب نعم، كيف سيحدث ذلك؟

ملاحظات



اسأل واستفسر

تحديد السلوك الشجاع وتعزيزه على الإنترنت

نظرة عامة على

النشاط 1: متى يجب طلب المساعدة
النشاط 2: الإبلاغ أيضًا على الإنترنت

المواضيع

من المهم أن يدرك الأطفال بأنهم ليسوا وحدهم عندما يرون محتوى على الإنترنت يُشعرهم بعدم الارتياح، وخاصةً إذا شعروا أن ذلك قد يعرضهم أو أشخاصًا آخرين للأذى. يجب ألا يترددوا أبدًا في طلب المساعدة من شخص يثقون به. من الجيد أيضًا أن يعرفوا أن هناك طرقًا مختلفة للتصرف بالشجاعة واتخاذ الخطوات، بدءًا من التحدث عن الأمور في الواقع والإبلاغ على الإنترنت.

الأهداف بالنسبة للطلاب

- ✓ فهم أنواع المواقف التي تستدعي طلب المساعدة أو التحدث مع شخص بالغ موثوق به
- ✓ التفكير في الخيارات المتاحة للتصرف بشجاعة وأهمية الحديث مع البالغين

المعايير ذات الصلة

معايير ISTE للمعلمين: 1c, 2c, 3a, 3b, 3c, 4b, 5a, 5b, 6a, 6b, 6d, 7a
معايير جامعة ISTE للطلاب لعام 2016: 1c, 2b, 3d, 4d, 6a, 7a, 7b, 7c
معايير AASL التعليمية: 2.a.1, 2.a.2, 2.a.3, 2.a.4, 2.b.1, 2.b.2, 2.b.3, 2.c.1, 2.c.2, 2.c.3, 2.d.1, 2.d.2, 2.d.3, 3.a.1, 3.a.2, 3.a.3, 3.b.1, 3.c.1, 3.c.2, 3.c.3, 3.d.1, 3.d.2, 3.d.3, 4.a.1, 4.a.2, 4.a.3, 4.b.1, 4.b.2, 4.b.3, 4.c.1, 4.c.2, 4.c.3, 4.d.1, 4.d.2, 4.d.3, 5.a.1, 5.a.2, 5.a.3, 5.b.1, 5.b.2, 5.b.3, 5.c.1, 5.c.2, 5.c.3, 5.d.1, 5.d.2, 5.d.3, 6.a.1, 6.a.2, 6.a.3, 6.b.1, 6.b.2, 6.b.3, 6.c.1, 6.c.2, 6.c.3, 6.d.1, 6.d.2, 6.d.3

اسأل واستفسر المفردات



شجاع جريء؛ ولكن ليس بالضرورة لا يعرف الخوف، لأن الأشخاص يظهرن الشجاعة بشكل خاص عندما يشعرون بالخوف أو التوتر ولكنهم يتصرفون بشكل إيجابي

حساب مُختَرَق: عبارة عن حساب على الإنترنت تم الاستيلاء عليه من قِبل شخص آخر بحيث لم يعد لديك السيطرة الكاملة عليه

مسؤولية الطلاب: خطوة تتعدى تعبير الطلاب عن آرائهم وتشمل قدرتهم على التصرف أو التغيير بما في ذلك حماية أنفسهم والآخرين والدفاع عنهم؛ وغالبًا ما تُعتبر هذه السمة عنصرًا جوهريًا من المواطنة

الثقة: الشعور بأن أمرًا ما أو شخصًا ما موثوق به أو صادق أو قادر على المساعدة

متى يجب طلب المساعدة

من النصائح التي تتكرر خلال هذه الدروس هي: إذا صادف الطلاب أمرًا يجعلهم يشعرون بالقلق أو ما هو أسوأ من ذلك، شجّعهم على الإبلاغ عنه، وأن يتحلوا بالشجاعة ويتحدثوا مع شخص يثقون به يمكنه المساعدة، بما في ذلك أنت أو مدير المدرسة أو أحد الوالدين. وفي حين أنه من المهم أن يفهم الطلاب هذه النقطة في كل واحد من الدروس، إليك مناقشة صافية تركز بشكل خاص على مبدأ "اسأل واستفسر" ليتربّخ في أذهانهم. ستجد في ما يلي قائمة بالحالات التي يمكن أن يساعد الحديث عنها.

ملاحظات مهمة للمعلم

1. لقد تم تعليم الأطفال أو تهيئتهم لـ "عدم الوشاية" على مدى عدة أجيال لدرجة أن هذا الأمر تحول إلى معيار اجتماعي، ويعمل خبراء الحماية من التنمر جاهدين لمساعدة الأطفال على فهم الفرق بين "الوشاية" وطلب المساعدة. ساعد طلابك على الفهم بأن طلب الدعم عند تعرضهم لمواقف مؤذية على الإنترنت لا يعتبر "وشاية"؛ بل يتعلق بطلب المساعدة لأنفسهم أو لأقرانهم عند التعرض للأذى.
2. يساهم تعزيز التواصل المفتوح في الصف وتذكير الطلاب بأنك موجود دائمًا لدعمهم في زيادة إحساسهم بالراحة والمسؤولية وتشجيعهم على الإبلاغ في الحالات المناسبة.
3. في المناقشة أدناه، في كل مرة يشارك فيها الطلاب أمثلة على مواقف طلبوا فيها المساعدة من شخص بالغ، تأكد من أنهم يتحدثون بنبرة تنم عن شعور بالفخر والشجاعة لقيامهم بذلك، خاصةً وأنهم يتحدثون أمام أقرانهم.

الأهداف بالنسبة للطلاب

- ✓ الإدراك بأن طلب المساعدة لأنفسهم أو للآخرين هو دليل على قوة
- ✓ التفكير ومناقشة المواقف التي يمكن أن يساعد فيها الحديث عن الأمر



دعونا نتحدث



في ما يلي قائمة من المواقف التي قد تصادفها على الإنترنت. قد لا نناقشها جميعها ولكنها أتمنى أن ترفعوا أيديكم عندما يذكركم أحد الأمور الواردة في القائمة بموقف مررتم به وكيف تصرفتم حياله، حتى تتمكن من التحدث عن هذه الحالات معًا.

إن طلب المساعدة عندما لا تكون متأكدًا مما يجب فعله هو تصرف شجاع، على الرغم من أنه قد لا يبدو كذلك دائمًا. وإذا ساعد هذا في التعامل مع موقف مؤذي أو الوقاية منه، فإنه تصرف ذكي وشجاع.

مواضيع النقاش



- 1. قراءة القائمة بصمت.** أثناء ذلك، فكروا إذا ما كنتم قد واجهتم أحد هذه المواقف، هل فكرتم في طلب المساعدة من شخص بالغ في أي منها، وهل طلبتم المساعدة؟
 - كان لديك شعور بأن حسابك قد تعرض للاختراق. (فكرة للنقاش: ما الذي يمكنك القيام به لتعزيز أمان حسابك؟)
 - احتجت إلى مساعدة في تذكر كلمة مرور.
 - لم تكن متأكدًا ما إذا كان أمر معين عبارة عن محاولة احتيال أو تعتقد أنك وقعت ضحية لمحاولة احتيال. (فكرة للنقاش: ما هي علامات التحذير؟)
 - حاول أحد الأشخاص مناقشة موضوع معك على الإنترنت جعلك تشعر بعدم الارتياح.
 - وصلتك رسالة أو تعليق مريب من شخص غريب. (فكرة للنقاش: ما الذي يجعل أمرًا ما مريبًا؟)
 - أردت مناقشة ملاحظة لطيفة جدًا أو فظة جدًا نشرها أحد الأشخاص على الإنترنت.
 - شعرت بالقلق من أنك ربما قد شاركت أمرًا ما على الإنترنت لم يكن ينبغي عليك مشاركته. أخبرنا ما هو الأمر إذا كنت تترتاح لمشاركته معنا، وفي جميع الحالات أخبرنا كيف تصرفت.
 - رأيت طالبًا يتعامل بفظاظة مع طالب آخر على الإنترنت.
 - رأيت شخصًا يهدد ببدء شجار أو إيذاء شخص ما.
 - قام شخص ما بنشر ملف شخصي مزيف منتحلًا شخصية طالب آخر.
 - كنت قلقًا بشأن طالب آخر بسبب أمر ما نشره أو أرسله في رسالة نصية. (فكرة للنقاش: أحيانًا يكون من الصعب المخاطرة بمضايقة صديقك، ولكن أليست سلامته أكثر أهمية؟)

2. ارفع يدك إذا كنت تريد إخبارنا بما فعلته (أو لم تفعله) ولماذا. إذا اختار شخص أحد المواقف، يمكنك اختيار موقف ملائم آخر للحديث عنه.

3. دعونا نقاش هذه المواقف.

ملاحظة للمشرفين

قد يساهم وجود لجنة طلاب أو مجموعة عمل في مدرستك (أو مدرسة إعدادية / ثانوية في منطقتك) بشكل كبير في تعزيز المسؤولية الطلابية تجاه هذا الموضوع. إذا كانت هناك بالفعل مثل هذه اللجنة أو المجموعة في مدرستك، اطلب من المستشارين مراجعة السيناريوهات المذكورة أعلاه مع الطلاب الأصغر سنًا ومشاركة تجاربهم الخاصة في التعامل معها.

اسأل واستفسر

الإبلاغ أيضًا على الإنترنت

باستخدام جهاز خاص بالمدرسة لإيضاح أين يمكن الإبلاغ عن محتوى وسلوك غير لائق في التطبيقات، يناقش الصف أنواعًا مختلفة من المحتوى ويقرر ما إذا كان يجب الإبلاغ عنها، ويناقش أيضًا أسباب الاختيار.

- ✓ التعرف على أدوات الإبلاغ عن الإساءة والمتوقّرة على الإنترنت
- ✓ معرفة متى يجب استخدامها
- ✓ التحدث عن الأسباب والحالات التي يجب فيها الإبلاغ عن إساءة

الأهداف بالنسبة للطلاب



دعونا نتحدث



عندما يظهر محتوى فظ أو غير لائق على الإنترنت، لدى الأشخاص عدة خيارات للتصرف. لقد ناقشنا في النشاط السابق أهم الخيارات وهو التحدث مع شخص تثق به. ولديك خيار آخر هو الإبلاغ عنه للتطبيق أو الخدمة حيث وجدت المحتوى ما قد يساعد على حذفه. من المهم الاعتماد على استخدام أدوات الإبلاغ على الإنترنت.

يجب أن يعتاد الطلاب على أخذ لقطة شاشة من المحادثات أو النشاط الضار أو المريب قبل استخدام أدوات الحظر والإبلاغ (الذي قد يجعل تسجيل النشاط غير متاح). هذا يضمن بأن يتمكن البالغون الموثوق بهم من رؤية ما حدث والمساعدة في إيجاد حل.

1. اكتشاف كيفية الإبلاغ عن مشكلة

احصل على أكبر عدد ممكن من الأجهزة التي يمكن لفك الوصول إليها، إذا كان هناك عدة أجهزة، قسّم الصف إلى مجموعات. ابحثوا معًا عن الأدوات في ثلاثة حسابات على الأقل تكون مرتبطة بالمدرسة للإبلاغ عن محتوى أو سلوك غير لائق. (إذا كان هناك جهاز واحد أو جهاز كمبيوتر واحد فقط في الغرفة، يمكن أن تتناوب مجموعات الطلاب على استخدام الجهاز).

2. الاطلاع على السيناريوهات

على كامل الصف الاطلاع على المواقف السبعة المذكورة في ورقة العمل.

3. هل ستبلغ عن هذا المحتوى؟

اطلب من الطلاب رفع أيديهم إذا كانوا سيبلغون عن المحتوى؛ ثم اطلب منهم رفع أيديهم إذا كانوا لن يبلغوا عن ذلك.

4. إذا كان الجواب نعم، لماذا؟

اطلب من طالب قد يبلغ عن المحتوى أن يشارك السبب مع الصف، واطلب من طالب لن يبلغ عن المحتوى شرح أسبابه.

ملاحظة: نادرًا ما يكون هناك إجابة أو تصرّف واحد صحيح. تأكد أن الطلاب يعرفون ذلك قبل بدء المناقشة في الصف.

النشاط



المواد المطلوبة:

* مستند ورقة عمل "الإبلاغ أيضًا على الإنترنت" يتم توزيعه على الطلاب

تحتوي معظم التطبيقات والخدمات على أدوات للإبلاغ عن المحتوى غير اللائق و/أو حظره، ويمكن للأشخاص المعنيين ومنتدياتهم والمنصات نفسها الاستفادة من استخدامنا لهذه الأدوات. قبل حظر المحتوى غير اللائق أو الإبلاغ عنه، من المفيد دائمًا حفظ لقطة شاشة حتى يكون لديك توثيق للموقف.

الإبلاغ أيضًا على الإنترنت

اقرأ كل واحد من السيناريوهات أدناه وارفع يدك إذا كنت ستبلغ عنه في التطبيق أو الخدمة التي عثرت عليها فيه. استعد لشرح سبب رغبتك في الإبلاغ عن هذا الأمر أو عدم الإبلاغ عنه وتوضيح أسباب اختيارك، ثم ناقش هذه الخيارات في الصف.

ملاحظة: يجب أن يدرك الجميع بأنه نادرًا ما يكون هناك اختيار واحد صحيح، وهذا ما يجعل المناقشة مفيدة. لا ينبغي لأحد أن يشعر بالسوء إزاء خياره. فالبالغون أيضًا لا يعرفون دائمًا متى أو كيف يجب الإبلاغ.

الموقف الأول

قام أحد الطلاب بنشر صورة جماعية في حساب عام وأنت غير راض عن مظهرك في هذه الصورة. هل تبلغ عن هذه الصورة أم لا؟ كيف يمكنك التعامل في مثل هذا الموقف؟

الموقف الثاني

أنشأ شخص حسابًا لطالب تعرفه مستخدمًا اسم الطالب وصورته. كما حول الصورة إلى مشاركة مضحكة ورسم شاربيًا وملامح وجه غريبة أخرى عليها، بحيث تحولت الصورة إلى مزحة. هل تبلغ عن هذا الحساب أم لا؟

الموقف الثالث

ينشر أحد الأشخاص الكثير من التعليقات المسيئة عن أحد الطلاب في مدرستك دون استخدام اسمه، ولكنك تشعر بأنك تعرفه. هل تبلغ عن هذه التعليقات أم لا؟

الموقف الرابع

أنشأ طالب حسابًا باسم مدرستك ونشر صور لطلاب مع تعليقات يمكن للجميع رؤيتها. كانت بعض التعليقات فظة وبعضها مجاملة. هل تبلغ عن التعليقات الفظة أو عن الحساب بأكمله أو عن كلاهما؟

الموقف الخامس

لاحظت أن طالبًا علّق على الإنترنت قائلاً إنه سيتشاجر مع طالب آخر في غرفة الطعام في اليوم التالي. هل تبلغ عن هذا التعليق على الإنترنت أم لا؟ هل تبلغ عنه إلى معلم أو المدير في صباح اليوم التالي أم لا؟ أو تبلغ عن التعليق بالشكلين؟

الموقف السادس

خلال مشاهدتك فيديو رسوم متحركة، يظهر فيه فجأة محتوى غريب ليس مناسبًا للأطفال يجعلك تشعر بعدم الارتياح. هل تبلغ عنه أم لا؟

الموقف السابع

خلال ممارستك للعبة على الإنترنت مع أصدقائك بدأ أحد الأشخاص الذين لا يعرفهم أي من اللاعبين بالدردشة معك. ومع أنه لم يزعجك بأي شكل من الأشكال، ولكنك لا تعرفه. هل تتجاهله أم تبلغ عنه؟

A series of horizontal lines intended for writing, spanning most of the page width.