

# חוכמה ערנות חוזק אדיבות אומץ



# גדולים באינטרנט

ברוכים הבאים לתוכנית הלימודים "גדולים באינטרנט", שנוצרה מתוך שיתוף פעולה בין Google ל-Internet Keep Safe Coalition (iKeepSafe.org). המשאב הזה הוא חלק מ"גדולים באינטרנט", תוכנית מגוונת שנועדה להקנות לילדים את הכישורים הדרושים להם כדי להתנהג בצורה בטוחה וחכמה באינטרנט.

תוכנית הלימודים "גדולים באינטרנט" מעניקה לנשות חינוך ולאנשי חינוך את הכלים ואת השיטות הנדרשים כדי ללמד בכיתה עקרונות בסיסיים של אזרחות דיגיטלית ובטיחות ברשת. מערכי השיעור עוסקים בנושאים החשובים ביותר, ומסייעים לנשות חינוך ולאנשי חינוך ללמד את התלמידים איך להיות אזרחים דיגיטליים מצליחים ובטוחים בעולם המרושת שלנו. השיעורים האלה מועשרים בטכניקות משחק (גיימיפיקציה) באמצעות "ממלכת האינטרנט" ([g.co/Interland](http://g.co/Interland)), משחק הרפתקאות מקוון. במשחק הזה לומדים על אזרחות דיגיטלית ובטיחות ברשת בצורה אינטראקטיבית ומהנה – כיאה לעולם האינטרנט.

חמישה נושאי יסוד של אזרחות דיגיטלית ובטיחות ברשת מגדירים איך להיות "גדולים באינטרנט":

- חושבים לפני שמשתפים (חכמים באינטרנט)
- זהירות, זיופים! (ערניים באינטרנט)
- שומרים על הסודות שלנו (חזקים באינטרנט)
- מגניב להיות אדיב (אדיבים באינטרנט)
- אם לא בטוחים, מדווחים (אמיצים באינטרנט)

השיעורים מתאימים בעיקר לכיתות ג' עד ו'. עם זאת, גם נשות חינוך ואנשי חינוך שמלמדים תלמידים צעירים ומבוגרים יותר נעזרים בתוכנית הלימוד, במיוחד בהקשר של אוצר מילים חשובות, דיונים בכיתה (שמותאמים לגיל הילדים) ומשחקים. אתם מוזמנים להתנסות כדי לגלות מה הכי מתאים לתלמידים שלכם – אפשר להעביר את כל תוכנית הלימודים מתחילתה ועד סופה, או להתעמק רק בשיעור אחד או שניים שהם החשובים ביותר לסביבה הלימודית שלכם.

האגודה הבינלאומית לשילוב טכנולוגיה בחינוך (ISTE) קיימה תהליך ביקורת בלתי תלוי על "גדולים באינטרנט", ובסופו הכירה בתוכנית כמשאב שמכין לומדים צעירים לעמוד בתקני ISTE 2016 לתלמידים. אגודת ISTE העניקה לתוכנית "גדולים באינטרנט" את האישור Seal of Alignment for Readiness.

תוכנית הלימודים "גדולים באינטרנט" והמשחק "ממלכת האינטרנט" הם שניים מתוך כמה משאבים שיכולים לעזור לבני משפחה, לנשות חינוך ולאנשי חינוך לעודד הרגלים נכונים לשימוש באינטרנט. לקבלת משאבים נוספים מ-Google, כמו סרטונים לימודיים לנשות חינוך ולאנשי חינוך, חומרי לימוד להורדה עבור הכיתה וכלים שימושיים לשילוב עם טכנולוגיה, ניתן להיכנס אל [g.co/BeInternetAwesome](http://g.co/BeInternetAwesome).





|    |                                                                                                                                                                                                                                                                             |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6  | <b>מדריך לנשות חינוך ולאנשי חינוך</b><br>משאב 1: תבנית למכתב/אימייל היכרות עבור ההורים<br>משאב 2: שאלות נפוצות                                                                                                                                                              |
| 10 | <b>שיעור 01: חושבים לפני שמשתפים</b><br>פעילות 1: מתי לא משתפים<br>פעילות 2: מנחשים את הפרופיל<br>פעילות 3: איך אנחנו נראים בעיני אחרים?<br>פעילות 4: איך לשמור על פרטיות<br>פעילות 5: ממלכת האינטרנט: הר הזהירות                                                           |
| 22 | <b>שיעור 02: זהירות, זיופים!</b><br>פעילות 1: אל תבלעו את הפיתיון!<br>פעילות 2: מי זה באמת?<br>פעילות 3: הבוטים האלה<br>פעילות 4: ממלכת האינטרנט: נהר האמת והשקר                                                                                                            |
| 40 | <b>שיעור 03: שומרים על הסודות שלנו</b><br>פעילות 1: איך יוצרים סיסמה מעולה<br>פעילות 2: שומרים על פרטיות<br>פעילות 3: ממלכת האינטרנט: מבצר הסיסמאות                                                                                                                         |
| 48 | <b>שיעור 04: מגניב להיות אדיב</b><br>פעילות 1: מעמדת הצופים מהצד לעמדת הצופים המתערבים<br>פעילות 2: אפשרויות לצופים המתערבים<br>פעילות 3: ...אבל תגידו את זה בצורה יפה!<br>פעילות 4: שימו לב לטון שלכם<br>פעילות 5: להתנהג בהתאם<br>פעילות 6: ממלכת האינטרנט: ממלכת האדיבות |
| 64 | <b>שיעור 05: אם לא בטוחים, מדווחים</b><br>פעילות 1: מתי כדאי לבקש עזרה<br>פעילות 2: מדווחים על זה, גם באינטרנט                                                                                                                                                              |

# מדריך לנשות חינוך ולאנשי חינוך: משאב 1

## תבנית מכתב/אימייל של היכרות להורים

זוהי תבנית בסיסית לאימייל או למכתב (שתוכלו לשנות לפי הצורך) שישלח להורים כדי להסביר להם איך כלים חדשים בתחום החינוך עוזרים לילדים שלהם לקבל החלטות נכונות לגבי הבטיחות וההתנהגות שלהם באינטרנט.

### הורים יקרים,



כשהילדים שלנו צעירים, אנחנו עושים כל מה שאנחנו יכולים כדי לעזור להם להפיק את מירב התועלת מהאינטרנט, ובמקביל מגינים עליהם מפני הסיכונים והחסרונות הקיימים בעולם המקוון. כשהילדים מתקרבים לגיל ההתבגרות, התפקיד שלנו משתנה: אנחנו מלמדים אותם להתנהל בעולם הדיגיטלי ולקבל בעצמם החלטות בטוחות ומתחשבות.

ב[שם בית-הספר] אנחנו מאמינים בשיתוף פעולה עם ההורים ובהכנת תלמידי [כיתה] כדי שיידעו:

- **לחשוב בצורה ביקורתית** ולבצע הערכה של אתרים, פוסטים, הודעות אימייל וכל תוכן אחר באינטרנט.

- **להגן על עצמם** מפני איומים באינטרנט, כולל בריונות ותרמיות.

- **לנהוג בחוכמה כשמשתפים:** מה, מתי, איך ועם מי לשתף.

- **להתנהג באדיבות ובכבוד** כלפי אנשים אחרים באינטרנט ולכבד את פרטיותם.

- **לבקש עזרה** מהורה או ממבוגר אחר שסומכים עליו, אם נתקלים במצבים מורכבים.

השנה החלטנו להכניס לבית הספר את "גדולים באינטרנט" - תוכנית מגוונת שנועדה להקנות לילדים את הכישורים הדרושים להם כדי להתנהג בצורה בטוחה וחכמה באינטרנט. אחד ממרכיבי התוכנית הוא המשחק המקוון "ממלכת האינטרנט", שדרכו הילדים יכולים לרכוש את הכישורים האלה בצורה אינטראקטיבית ומהנה - ממש כמו האינטרנט עצמו. התוכנית "גדולים באינטרנט" פותחה על ידי Google בשיתוף עם נשות חינוך ואנשי חינוך, חוקרים ומומחים לבטיחות באינטרנט מ-iKeepSafe.org. היא משלבת חוויות לימוד מהנות המותאמות לגילאים שונים, ומחולקת לחמישה שיעורים בסיסיים:

- **חושבים לפני שמשתפים**
- **זהירות, זיופים!**
- **שומרים על הסודות שלנו**
- **מגניב להיות אדיב**
- **אם לא בטוחים, מדווחים**

שימוש מושכל ובטוח בטכנולוגיה יקדם את הלמידה העצמאית של התלמידים, וישפר את פעילותו של בית הספר שלנו. מטרתנו היא להבטיח שכל תלמידי [שם בית-הספר] לומדים, חוקרים ושומרים על בטיחות באינטרנט, בין כותלי בית הספר ומחוץ לו. אנחנו סבורים שהתוכנית "גדולים באינטרנט" היא שלב חשוב בדרך להשגת היעד הזה.

נשמח לשתף איתכם מידע נוסף על התוכנית החדשה, ולהציג כמה מחומרי הלימוד ומקורות המידע שישמשו את התלמידים בכיתה. אתם גם מוזמנים לעיין בחומרים ובמקורות המידע למשפחות בכתובת: [g.co/BelInternetAwesome](http://g.co/BelInternetAwesome). מומלץ לשאול את הילדים שלכם על הפעילויות שהם משתתפים בהן, ולהמשיך את השיחה בבית - מי יודע, אולי תלמדו מהם כמה טריקים לגבי פרטיות ואבטחה!

בברכה,

[השם שלכם]

## שאלות נפוצות

### האם צריך להשלים את השיעורים לפני שמשחקים ב"ממלכת האינטרנט"?

לא חובה, אבל אנחנו ממליצים ללמד את השיעורים לפני שמשחקים ב"ממלכת האינטרנט". המשחק יעיל יותר כשהוא מחזק את הנושאים שתוארו בתוכנית הלימוד, והוא מהנה יותר לאחר שהתלמידים מנהלים דיונים וסיעור מוחות עם המורים.

### האם התלמידים צריכים חשבונות Google לתוכנית "גדולים באינטרנט"?

לא! התוכנית זמינה לכל מי שנכנס לאתר. אין צורך בהתחברות, בסיסמאות ובכתובות אימייל.

### באילו מכשירים אפשר לשחק ב"ממלכת האינטרנט"?

המשחק "ממלכת האינטרנט" עובד בכל מכשיר שיש לו חיבור לאינטרנט ודפדפן אינטרנט. כלומר, רוב המחשבים הנייחים, המחשבים הניידים, הטאבלטים והטלפונים הניידים יכולים לעזור לכם להיות גדולים באינטרנט.

### מהן כתובות ה-URL החשובות?

- דף הבית של "גדולים באינטרנט": [g.co/BelInternetAwesome](http://g.co/BelInternetAwesome)
- משחק "ממלכת האינטרנט": [g.co/Interland](http://g.co/Interland)
- תוכנית הלימודים של "גדולים באינטרנט": [g.co/BelInternetAwesomeCurriculum](http://g.co/BelInternetAwesomeCurriculum)

### האם נדרשת הכשרה מיוחדת למורים כדי ללמד את התוכנית? או שצריך להיות בעל אישיות מיוחדת?

- קודם כול, כל גננת בגן חובה וכל מורה מכיתה א' ועד כיתה י"ב יכולים להעביר את תוכנית הלימודים הזו לתלמידים שלהם. לא נדרשת הכשרה נוספת.
- ועוד משהו: בכל מורה יש משהו מיוחד. (:

### לאילו כיתות התוכנית "גדולים באינטרנט" הכי מתאימה?

התוכנית המלאה, שכוללת את תוכנית הלימודים, המשחק והמשאבים באתר, נועדה למשתמשים בכיתות ג' עד ו' (גילאים 8 עד 12). עם זאת, המורים יכולים להתאים את תוכנית הלימודים כך שהנושאים יועילו לכל שכבת גיל.

### איך ילדים לומדים מהמשחק?

באמצעות המשחק, הילדים מגלים בחופשיות שיטות עבודה נכונות, ומבינים אינטראקציות בדיגיטל – ואת ההשלכות שלהן – במרחב בטוח ובסביבה חינוכית. כך המשחק מחזק מושגים מתוכנית הלימודים.

### האם אפשר להשתמש בכל אחד מהשיעורים ב-Google Classroom?

כן, בטח. ניתן להקצות את המשחק "ממלכת האינטרנט" לכיתות או לקבוצות מסוימות, או לפתוח אותו לכל התלמידים באמצעות class announcement (הכרזה בכיתה).

**האם יש אתר או תיקייה משותפים עם דפי עבודה שניתן לגשת אליהם בקלות כדי להקריין במצגת על לוח?**

כן, יש אוספים של מצגות. כדי להציג את העדכון האחרון בתוכנית "גדולים באינטרנט", פעלנו בשיתוף עם Pear Deck להתאמת תוכנית הלימודים למצגות כדי להציג, להפיץ ולשתף בקלות. כאן תוכלו למצוא אותן: [beinternetawesome.withgoogle.com/en/resources](https://beinternetawesome.withgoogle.com/en/resources).

**האם אנחנו צריכים להיות מומחים לאזרחות דיגיטלית כדי להשתמש בתוכנית?**  
בכלל לא. תוכנית הלימודים תוכננה כך שכל מורה יוכל להיעזר בה וללמד אותה בכיתה. אם אתם רוצים לרענן את הידע או לקבל מידע נוסף על אזרחות דיגיטלית ובטיחות, תוכלו ללמוד את הקורס המקוון שלנו לנשות חינוך ולאנשי חינוך בכתובת: [edutrainingcenter.withgoogle.com/digital\\_citizenship/preview](https://edutrainingcenter.withgoogle.com/digital_citizenship/preview).

**האם תוכנית הלימודים של "גדולים באינטרנט" מותאמת לתקנים כלשהם?**  
טוב ששאלתם. כן. בטח. התוכנית "גדולים באינטרנט" מותאמת לתקנים של האגודה הבינלאומית לשילוב טכנולוגיה בחינוך (ISTE) ושל האיגוד האמריקאי של ספרנים בבתי-ספר (AASL).

**האם התלמידים יכולים לשמור את המהלכים שלהם במשחק "ממלכת האינטרנט"?**  
לא בגרסה הנוכחית, וכנראה שזה לא ישתנה. במסגרת "גדולים באינטרנט", לא נוצרים ולא מאוחסנים פרטים אישיים מזהים כלשהם, כולל קבצים שמורים. כך זה תוכנן מראש – רצינו שהחווייה תהיה נגישה לכולם ולכן לא נדרשים חשבון, התחברות או סיסמה.

**יפה, אבל יש לי תלמידים רבים שגאים במה שהם למדו ושסיימו את המשחק.**  
אנחנו מבינים, ולכן יצרנו תבנית שאפשר להפיק ממנה ולהדפיס תעודת סיום אישית. פשוט מכניסים את שם התלמיד.

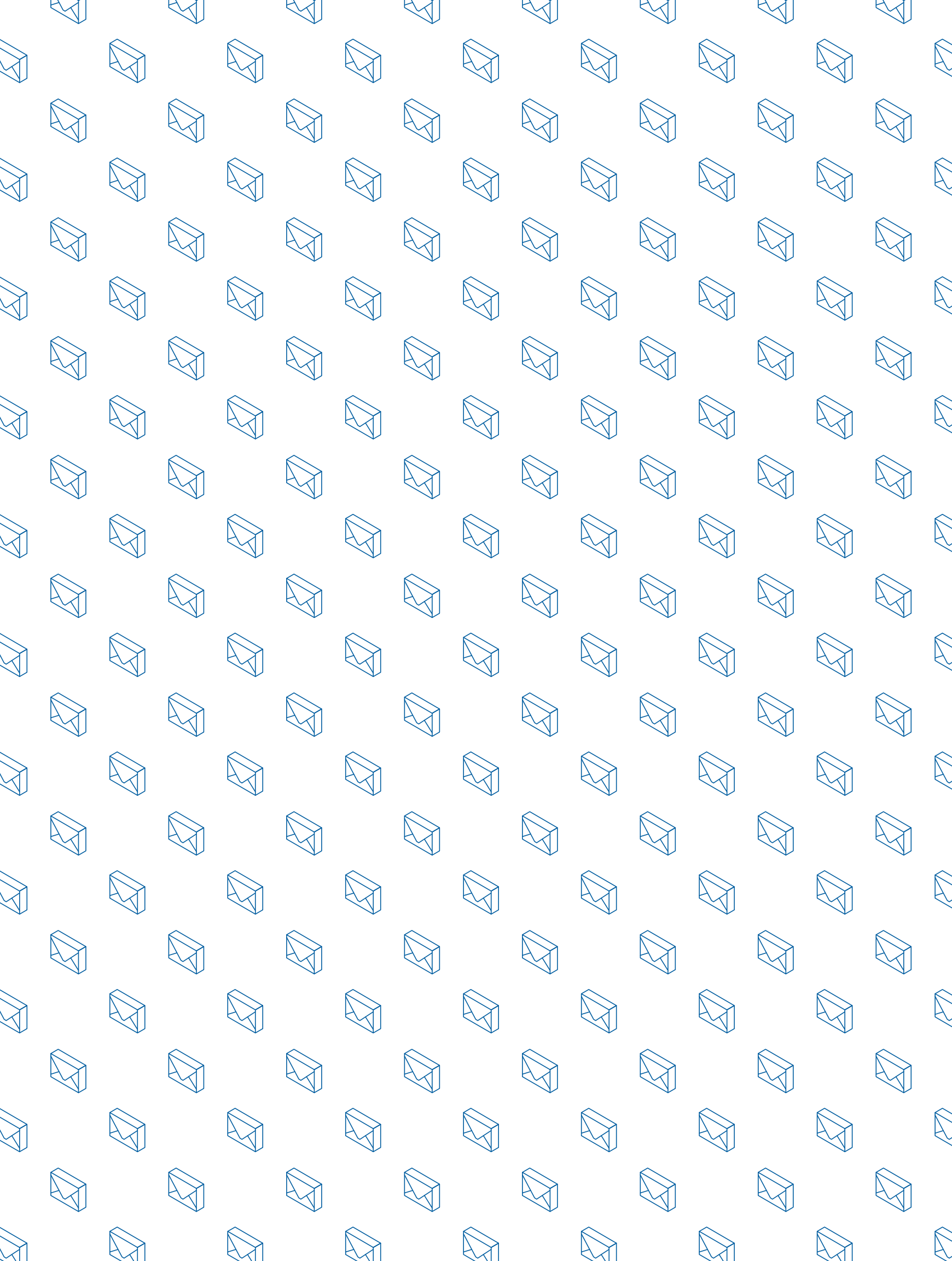
**איפה אפשר למצוא את המשאבים הנוספים לנשות חינוך ולאנשי חינוך?**  
ניתן למצוא את כל החומרים של תוכנית "גדולים באינטרנט" לנשות חינוך ולאנשי חינוך בכתובת: [beinternetawesome.withgoogle.com/en/resources](https://beinternetawesome.withgoogle.com/en/resources).

**האם יש קהילה מקוונת של משתמשי "גדולים באינטרנט" שבה אפשר לשתף רעיונות או לקבל עזרה?**

כן! (והיא נהדרת.) אנחנו משתמשים בדף הטוויטר שלנו כדי לנהל תקשורת שוטפת עם מורים ולהציע להם רעיונות. כדי לדעת יותר על "גדולים באינטרנט" ועל נושאים נוספים, בואו לעקוב אחרינו ב- [@GoogleForEducation](https://@GoogleForEducation).



## הערות



# חושבים לפני שמשתפים

איך להגן על עצמכם ועל המוניטין שלכם באינטרנט

## סקירה כללית של השיעור

- פעילות 1: מתי לא משתפים
- פעילות 2: מנחשים את הפרופיל
- פעילות 3: איך אנחנו נראים בעיני אחרים?
- פעילות 4: איך לשמור על פרטיות
- פעילות 5: ממלכת האינטרנט: הר הזהירות

## הרעיונות העיקריים

מורים והורים מבינים שטעויות שעושים בשלב מוקדם בעולם הדיגיטלי עלולות לפגוע ברגשות, במוניטין ובפרטיות. אבל ילדים יכולים לכתוב פוסט שנראה להם בלתי מזיק היום, ויהיה קשה לשכנע אותם שאנשים שהם לא חשבו שיראו את הפוסט, יפרשו אותו בצורה לא נכונה מחר, ועל אחת כמה וכמה בעתיד.

בפעילויות האלה נשתמש בדוגמאות קונקרטיות וניזום דיונים מעוררי-מחשבה כדי ללמד תלמידים איך לנהל את הגדרות הפרטיות ולהגן על המידע האישי שלהם, כדי שיהיה להם פרופיל מקוון חיובי.

## יעדים לתלמידים

- ✓ ליצור ולנהל מוניטין חיובי באינטרנט ובמקומות אחרים.
- ✓ לכבד את גבולות הפרטיות של אחרים, גם אם הם שונים מהגבולות שלכם.
- ✓ להבין את ההשפעה הפוטנציאלית של טביעת רגל דיגיטלית שאינה מנוהלת כראוי.
- ✓ לבקש עזרה ממבוגרים אם מתמודדים עם מצבים מורכבים.

## תקנים רלוונטיים

תקני ISTE לנשות חינוך ולאנשי חינוך: 1a, 1b, 2a, 2c, 3b, 3c, 3d, 4b, 4d, 5a, 6a, 6b, 6d, 7a  
תקני ISTE לתלמידים 2016: 1c, 1d, 2a, 2b, 2d, 3b, 3d  
תקני למידה של AASL: 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, II.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

# חושבים לפני שמתפנים

## אוצר מילים



**פרטיות באינטרנט:** מונח רחב שמתייחס בדרך כלל ליכולת לשלוט בסוג המידע שאתם משתפים על עצמכם באינטרנט, מי יכול לראות את המידע ולשתף אותו

**טביעת רגל דיגיטלית (או נוכחות דיגיטלית):** כל המידע האישי שלכם שמופיע באינטרנט. היא יכולה לכלול כל דבר, החל מתמונות, קטעי שמע, סרטונים והודעות טקסט ועד לייקים ותגובות שאתם מפרסמים בפרופילים של חברים. בדיוק כמו שהצעדים שלכם משאירים עקבות על האדמה כשאתם הולכים, גם התוכן שאתם מפרסמים באינטרנט יוצר טביעת רגל.

**מוניטין:** הרעיונות, הדעות, ההתרשמות או האמונות שיש לאחרים לגביכם. משהו שאתם לא יכולים לדעת בביטחון גמור, אבל רוצים שהוא יהיה חיובי

**מידע אישי:** מידע אישי או רגיש הוא מידע שמאפשר לזהות אדם מסוים, לדוגמה: שם, כתובת מגורים, מספר הטלפון, מספר תעודת זהות, כתובת אימייל, מספר כרטיס אשראי וכו'. כדאי לחשוב טוב לפני שמתפנים מידע כזה באינטרנט.

**שיתוף יתר:** שיתוף מוגזם - כשמישהו משתף יותר מדי מידע אישי או יותר מדי מידע על עצמו במצב מסוים או בשיחה באינטרנט.

**הגדרות:** זהו האזור בכל מוצר דיגיטלי, אפליקציה, אתר וכו', שבו אפשר להגדיר מה אתם משתפים, איך לנהל את החשבון שלכם ומהן הגדרות הפרטיות שלכם.

# חושבים לפני שמשתפים: פעילות 1

## מתי לא כדאי לשתף

התלמידים עובדים בזוגות ומספרים זה לזה סודות מומצאים. המטרה היא להתחיל לחשוב איזה מידע הוא פרטי ומהם גבולות הפרטיות.

### יעדים לתלמידים



- ✓ להבין אילו סוגים של מידע אישי צריכים להיות פרטיים.
- ✓ לזכור שצריך לכבד את ההחלטות של כל האנשים לגבי פרטיותם.

### בואו נדבר



#### למה הפרטיות חשובה?

טביעת הרגל הדיגיטלית שלכם מייצגת אתכם באינטרנט. התוכן יכול לכלול תמונות, אודיו, סרטונים, הודעות טקסט, לייקים ותגובות שאתם מפרסמים בפרופילים של חברים. בדיוק כמו שחשוב לשמור על נוכחות חיובית בעולם הפיזי האמיתי (למשל בית-הספר), חשוב שהנוכחות שלכם תהיה חיובית גם באינטרנט.

האינטרנט מאפשר לתקשר בקלות עם בני משפחה, חברים ואנשים בעלי תחומי עניין דומים שלכם. אנחנו שולחים הודעות, משתפים תמונות ומצטרפים לשיחות ברשתות חברתיות, ולפעמים אנחנו לא חושבים מי עוד יכול לראות את המידע הזה. קחו למשל תמונה או פוסט שנראים לכם היום משעשעים ובלתי מזיקים. מתישהו בעתיד אנשים שבכלל לא רציתם שיראו אותם עלולים לראות ולפרש אותם בצורה שגויה. יש דברים שעדיף לשתף באופן אחר, למשל בשיחת טלפון או פנים אל פנים. כשמשהו מתפרסם באופן ציבורי, כמעט אין דרך חזרה. חשוב לזכור:

- כמו כל דבר אחר באינטרנט, טביעת הרגל שלכם חשובה לאנשים שלא פגשתם.
- כשתוכן שכתבתם או תוכן שקשור אליכם מתפרסם באינטרנט, הוא יכול להישאר שם לנצח. זה כמו טוש סימון: אי אפשר למחוק את מה שכתבתם בו, גם אם תבינו שרציתם לכתוב משהו אחר.

לכן הפרטיות שלכם חשובה. כדי להגן עליה, אתם יכולים להחליט שתשתפו רק דברים שאתם בטוחים שאתם רוצים לשתף – במילים אחרות, לפרסם ולשתף באינטרנט בזהירות. איזו סיבה אחרת יכולה להיות לחשיבות הרבה של הפרטיות?

חשוב גם לדעת מתי לא לפרסם כלום – לא להגיב לפוסט, לתמונה או לתגובה של מישהו, או לא לשתף מידע שאינו נכון. כולם כבר מכירים את העצה הכי טובה שיש: "חושבים לפני שמפרסמים". כדי לכבד את הפרטיות שלכם ושל אנשים אחרים, צריך לחשוב מה נכון לפרסם, מי יכול לראות את הפוסט, מה עשויה להיות ההשפעה עליכם ועל אחרים, מתי כדאי לפרסם ומתי לא כדאי.

שאלות לדיון נוסף (התלמידים יכולים לקחת איתם שאלות הביתה כדי לדון בהן עם בני משפחה):

- מתי אפשר לשתף תמונה או סרטון של אדם אחר?
- למה כל כך קשה לשמור סודות?
- האם אפשר לחשוף סוד של אדם אחר?
- ואם האדם הזה הוא מישהו שאכפת לכם ממנו, והוא מפרסם תוכן שלדעתכם מעיד על כך שהוא בסכנה? אם לדעתכם אתם צריכים לשתף את הסוד הזה, האם עליכם לגלות לו שאתם חושבים על כך לפני שאתם עושים משהו? האם עליו לדעת שאתם מודאגים?



### 1. ממציאים סוד

בשלב הראשון, כל אחד ממציא דמות (ילד או ילדה) שיש לה סוד.

### 2. מספרים לבן/בת הזוג

חשבתם על סודות? בשלב זה מתחלקים לזוגות, כל אחד מספר לבן/בת הזוג על הדמות המומצאת והסוד שלה, והם דנים בשלוש השאלות הבאות:

- לוו הייתם במקומה של הדמות, האם הייתם משתפים את הסוד הזה עם כל אחד?
- עם מי הייתם משתפים את הסוד שלכם ומדוע?
- איך הייתם מרגישים אם מישהו היה מגלה את הסוד שלכם לכולם בלי רשותכם?

### 3. מספרים לכיתה

לסיום, כל תלמיד מספר לכיתה מהי הדמות שהמציא ומה הסוד שלה, ומתאר איך הרגיש כשהוא שיתף אותו. תלמידי הכיתה יכולים לדון בתשובות שלהם לשאלות שלמעלה.

### מה למדנו?

סודות הם סוג אחד של מידע אישי שייתכן שלא נרצה לגלות לאחרים, או שנרצה לשתף רק עם בני משפחה או חברים שאנחנו סומכים עליהם. אחרי שמשתפים סוד, כבר אין לנו שליטה עליו והוא עלול להתגלות לאנשים הלא רצויים. על אילו סוגי מידע נוספים כדאי לנו להגן?

- הכתובת ומספר הטלפון שלכם
- כתובת האימייל
- הסיסמאות שלכם
- שמות המשתמשים
- שיעורי הבית שלכם ומסמכים אחרים שאתם יוצרים

## חושבים לפני שמשתפים: פעילות 2

# מנחשים את הפרופיל

התלמידים בוחנים אוסף של פרטים אישיים על דמות בדויה, כדי לנסות להסיק מסקנות לגבי אותו אדם.

### יעדים לתלמידים



- ✓ לזהות דרכים למציאת מידע על אנשים באינטרנט.
- ✓ לחשוב איך אנשים מגבשים דעה על מישהו על סמך התוכן שהוא מפרסם באינטרנט.
- ✓ להעריך עד כמה המידע מדויק ולזהות את ההבדלים בין הנחות, דעות ועובדות.

### בואו נדבר



#### איך אנחנו יודעים את מה שאנחנו (חושבים שאנחנו) יודעים

- אפשר למצוא הרבה מידע אישי באינטרנט. חלק מהמידע הזה יכול לגרום לנו להניח הנחות שגויות לגבי אנשים. נחקור את הנושא באמצעות השאלות הבאות:
- מה אנחנו יכולים ללמוד על אדם מסוים מהמידע האישי שלו?
  - מה אנחנו יכולים לנחש מהמידע האישי, אפילו אם אנחנו לא בטוחים?
  - האם אנחנו יודעים איך המידע הזה נאסף מלכתחילה? איך אפשר לזהות את המקור?

### פעילות



#### 1. לומדים על האדם

אם תחליטו להשתמש בסיפורים ובדמויות שבדף העבודה, כל אחד יקבל עותק לקריאה. אם תחליטו להשתמש בדמויות ובסיפורים שהמציאו התלמידים, בחרו שלוש דמויות וכתבו את הפרטים שלהן ברשימות כמו בדף העבודה. חשוב לוודא שכל אחד יקבל עותק משלו ויקרא אותו.

#### 2. כותבים תיאור

מתחלקים לקבוצות, לכל קבוצה יש דמות אחת/אדם אחד. כל קבוצה כותבת תיאור קצר של האדם הזה. מי אתם חושבים שהוא?

#### 3. חושפים את האמת

עכשיו נגלה את האמת על הדמויות (זכרו לחכות ולקרוא את המידע רק לאחר שהקבוצות סיימו לכתוב את התיאור):

- **טלי** היא תלמידת י"ב. היא תגייס בקיץ, ובהמשך מקווה ללמוד הנדסה כימית באוניברסיטה. החלום שלה הוא להקים חברה משלה. מה הכי חשוב לה: משפחה, התנדבות, תרבות פופ, אופנה.
- **דנה** היא שחקנית כדורסל בנבחרת של בית הספר התיכון שלה. היא בת 15 וגרה בראשון לציון. יש לה אחות בת 8. מה הכי חשוב לה: כדורסל, אומנות, לנגן בגיטרה, לבלות עם החברים
- **אייל** בן 14. הצטרף לא מזמן לנבחרת הכדורגל. יש לו שני חתולים. הוא מוכשר בציור ואוהב לבנות רובוטים. מה הכי חשוב לו: טכנולוגיה, קבוצת הכדורגל שלו, בעלי חיים וזכויות של בעלי חיים

#### 4. מתחילים בדיון

עכשיו נבדוק אילו מהניחושים שלנו היו נכונים ואילו היו שגויים. למה כן ולמה לא? מה למדנו מהפעילות הזו?

#### החומרים הדרושים:

- סיפורים על פעילויות באינטרנט של כמה דמויות מומצאות או אנשים אמיתיים. אפשר לחלק את דף העבודה "מנחשים את הפרופיל". לחלופין, כעבודת כיתה או כשיעור בית לבדיקה למחרת, ניתן לאסוף דוגמאות באמצעות הרעיונות הבאים:
- חשבונות של בני משפחה או ידוענים ברשתות חברתיות, בהתאם לגיל
- יומנים מודפסים של היסטוריית השימוש בדפדפן
- מחברות או מכשירים למשימת כתיבה קצרה

כשאנחנו רואים פוסטים, תגובות ותמונות של אנשים, אנחנו מניחים לגביהם הנחות שלא תמיד נכונות, במיוחד אם אנו לא מכירים אותם. הסיבה לכך היא שהפרטים שרואים באינטרנט הם רק חלק ממי שהם וממה שחשוב להם. ייתכן גם שהם מתחזים למישהו, או שזה מה שהם מרגישים רק ברגע שבו הם מפרסמים. אי אפשר לדעת באמת מיהם או איך הם מרגישים עד שמכירים אותם באופן אישי, וגם לאחר מכן, לוקח זמן להכיר טוב!



## דף עבודה: פעילות 2

# מנחשים את הפרופיל

קראו למטה כל אחד מהתיאורים של פעילות מקוונת של אדם מסוים. על סמך הפרטים שאתם רואים כאן, כתבו תיאור קצר על האדם הזה: מה הוא אוהב, לא אוהב ומה הכי חשוב לו?

### אייל

היכל ההמבורגרים של דוד 

החטאנו את שער הניצחון. אוף.  
לפחות היה תיקו.

25 תמונות של כלבלבים 

מסיבת פורים בתיכון בליך 

מה דעתכם על האתר של חברה שלי?  
אני כתבתי חלק גדול מהקוד שלו.

שיא חדש!!  
כאן... אני מת על ג'ם ג'ם!!

### דנה

ניצחנו במשחק! נותר עוד משחק אחד לפני  
האליפות. חייבת להתאמן עוד על זריקות  
מה-3.

אני שונאת מסיבות ריקודים בבית הספר.  
#לא\_הולכת

האקדמיה למדע, ראשון לציון 

10 סימנים שההורים שלך מנסים  
להרוס לך את החיים 

הולכת בשבת לדוג עם אבא שלי  
בקיסריה! כיף מטורף

לה לה לונה במרכז העיר 

### טלי

תמונות תת-ימיות מהנשף! מהממים  
שאתם!

השיטות הטובות ביותר לרפא  
חצ'קונים 

אחי הקטן אלכס כזה מעצבן. אולי הוא חייזר

קנס על מהירות 

כנס מעצבים צעירים בשנקר 

סוף סוף ראיתי את הסרט החדש של  
מלחמת המרגלים. OMG טירוף!

# חושבים לפני שמשתפים: פעילות 3

## איך אנחנו נראים בעיני אחרים?

התלמידים בודקים איך הדמות מהפעילות הקודמת תיראה בעיני סוגים שונים של אנשים – הורים, מעסיקים, חברים, שוטרים.

### יעדים לתלמידים



- ✓ להבין את נקודות המבט של אנשים אחרים כשאנחנו מנסים להחליט אם לשתף מידע באינטרנט.
- ✓ לשקול את ההשלכות של חשיפת מידע אישי: מה שתתפזר יהפוך לחלק מהמוניטין שלכם, ועלול ללוות אתכם זמן רב.
- ✓ לפתח יעד: ליצור באופן פעיל נוכחות חיובית באינטרנט.

### בואו נדבר



#### נקודת מבט חדשה

מתוך המידע בטביעת הרגל הדיגיטלית שלכם, אנשים יכולים לגלות פרטים רבים יותר ממה שהתכוונתם לחשוף – ועלולות להיות לכך השלכות משמעותיות.

בואו נבחן שוב את הפרופיל מנקודת המבט של הדמות שלנו.

- האם לדעתכם הדמות הזו רוצה שאנשים יידעו את כל המידע האישי הזה? למה כן ולמה לא?
- אילו סוגי אנשים היא הייתה רוצה שיראו זאת ואילו לא?
- איך המידע הזה עשוי להיראות לאחרים?
- איך אנשים אחרים עשויים להשתמש במידע הזה?

במצבים שונים נדרשות רמות שונות של פרטיות. המפתח להרגלי פרטיות נכונים באינטרנט הוא לחשוב איך אני רואה את עצמי ואיזה רושם אחרים יקבלו עליי בעקבות מה שפרסמתי.

### פעילות



#### 1. מסתכלים מנקודת מבט חדשה

עכשיו נתחלק לקבוצות, וכל קבוצה תחשוב על הדמות שלנו מנקודת המבט של אחד מסוגי האנשים הבאים:

- |                    |        |         |
|--------------------|--------|---------|
| • הורה             | • מאמן | • מעסיק |
| • חבר              | • שוטר | • מפרסם |
| • אתם בעוד 10 שנים |        |         |

מה חשוב לכם בתור הורה, מאמן, מנהל, חבר וכן הלאה? אילו מסקנות הם יסיקו לגבי הדמות? איך הם ישתמשו במידע הזה? מחקו את המידע שאתם חושבים שהדמות שלנו לא הייתה רוצה שתראו.

#### 2. מציגים את המסקנות

כל קבוצה מציגה את התוצאות שלה ומסבירה את הבחירות שעשתה לגבי הפרטיות. זו יכולה להיות הזדמנות טובה למשחקי תפקידים, אם תלמידי הכיתה מעוניינים בכך.

#### 3. דיון בכיתה

מהן הנקודות החשובות ביותר שלמדתם מהפעילות הקבוצתית הזו? למה מהמידע שבדקנו עלול להתגבש סיפור חלקי? מהן לדעתכם ההשלכות של מצב שבו אדם מגבש דעה שלילית עליכם, על סמך המידע שנמצא באינטרנט?

#### החומרים הדרושים:

- כל תלמיד יקבל עותק של הפרופילים המומצאים מפעילות 2

אנשים שונים יכולים לראות את אותו המידע ולהסיק ממנו מסקנות שונות. אל תניחו שאנשים באינטרנט יראו אתכם כפי שאתם חושבים שהם יראו אתכם.

## חושבים לפני שמשתפים: פעילות 4

# שומרים על פרטיות

תלמידי הכיתה סוקרים ארבעה תרחישים כתובים, ודנים בפתרון הפרטיות הטוב ביותר לכל אחד מהם.

### יעדים לתלמידים



- ✓ לבחון איך סוגיות של פרטיות נראות מנקודות המבט של אנשים שונים.
- ✓ להבין איך תרחישים שונים מחייבים רמות שונות של פרטיות.

### בואו נדבר



#### תרחישי פרטיות: מה אתם צריכים לעשות?

**תרחיש 1:** ילדה שאתם מכירים בבית הספר נעקצה על ידי חרק מוזר ויש לה עכשיו פריחה מכושרת בבטן. היא לא רוצה שאנשים אחרים יידעו על כך.

- האם יש לאנשים אחרים זכות לדעת?
- האם אתם צריכים להיות אלה שיספרו להם?

**תרחיש 2:** מישהי כותבת ביומן האישי שלה. אדם אחר מעתיק את מה שהיא כתבה ומפרסם את זה באינטרנט.

- האם האדם האחר שגה כשפרסם את הכתוב ביומן?
- איך הייתם מרגישים אם מישהו היה פועל כך לגבי מידע שרציתם לשמור בפרטיות?

**תרחיש 3:** מישהו מפרסם את הפוסט "חופשה נעימה" בדף של חבר במדיה חברתית.

- האם החבר הודיע באופן ציבורי שהוא יוצא לחופשה? האם הוא רצה שכולם יידעו?
- האם יש דרכים פרטיות יותר להעביר את ההודעה – למשל, לשלוח הודעת SMS או בווטסאפ?

**תרחיש 4:** אתם יודעים שתלמיד יצר חשבון מזויף ברשת החברתית, הוא התחזה לתלמיד אחר בצורה שלילית וכלל את המידע האישי שלו.

- האם לתלמיד יש זכות לדעת?
- האם מישהו צריך לספר על כך למורה או למבוגר אחר שסומכים עליו? איך? מה עלול לקרות אם אף אחד לא יספר?
- לא ברור מי יצר את החשבון, אבל אתם יודעים. האם אתם צריכים למסור את המידע הזה למבוגר שסומכים עליו?

### פעילות



נסקור את ארבעת התרחישים, ונדבר על כך שלכל אחד מהם יכול להיות פתרון פרטיות שונה. נתחלק לארבע קבוצות, כל קבוצה תדון בתרחיש אחד. לאחר מכן, נערוך דיון כיתתי על הממצאים שלנו.

### מה למדנו?

במצבים שונים נדרשות תגובות שונות, באינטרנט ובמקומות אחרים. תמיד חשוב לכבד את בחירות הפרטיות של אנשים אחרים, גם אם אתם הייתם בוחרים אחרת.

## חושבים לפני שמשתפים: פעילות 5

# ממלכת האינטרנט: הר הזהירות

מרכז העיירה ההררי של ממלכת האינטרנט הוא המקום שבו כולם נפגשים עם כולם. עליכם לחשוב טוב מה אתם רוצים לשתף ועם מי. המידע נע במהירות האור, ואחד הרשתונים שאתם מכירים הוא שתפניסט.

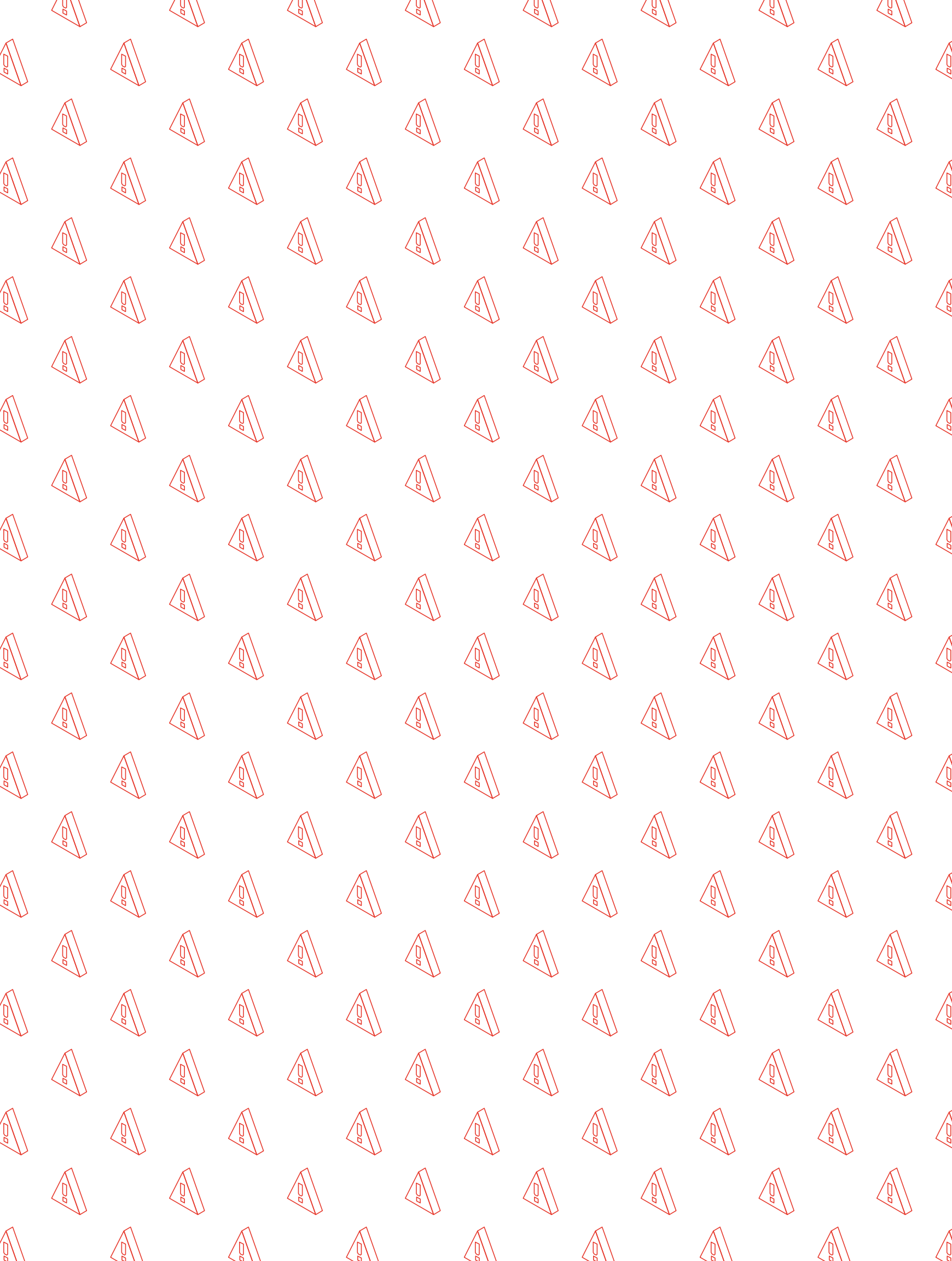
יש לפתוח דפדפן אינטרנט במחשב או בנייד שלכם (לדוגמה, בטאבלט) ולהיכנס אל [g.co/MindfulMountain](http://g.co/MindfulMountain).

### נושאים לדיון



התלמידים ישחקו ב"הר הזהירות", ובעזרת השאלות הבאות ידונו במה שהם למדו מהמשחק. רוב התלמידים מפקים את מירב התועלת ממשחק עצמאי, אבל התלמידים יכולים גם לשחק בזוגות. זה יכול לעזור במיוחד לתלמידים צעירים.

- מתוך כל הפוסטים ששיתפתם במשחק, איזה סוג לדעתכם תשתפו הכי הרבה במציאות? למה?
- תארו מצב שבו שיתפתם בטעות מידע שלא הייתם צריכים לשתף.
- למה לדעתכם הדמות בהר הזהירות נקראת "שתפניסט"?
- תארו את אופי השתפניסט ואיך הפעולות שלו משפיעות על המשחק.
- האם המשחק בהר הזהירות שינה את אופן החשיבה שלכם לגבי שיתוף עם אחרים באינטרנט בעתיד?
- תארו פעולה אחת שתעשו אחרת בעקבות השיעורים האלה וההתנסות במשחק הזה.
- תנו דוגמה אחת להשלכה שלילית בעקבות שיתוף ציבורי, בהשוואה לשיתוף עם החברים בלבד.
- מה אפשר לעשות אם משתפים בטעות פרטי? מה קורה אם מישו משתף איתכם בטעות פרטי מדי?



# זהירות, זיופים!

## איך להיזהר מדיוג (פישניג) ומתרמיות

### סקירה כללית של השיעור

- פעילות 1: אל תבלעו את הפיתיון!
- פעילות 2: מי זה באמת?
- פעילות 3: הבוטים האלה
- פעילות 4: ממלכת האינטרנט: נהר האמת והשקר

### הרעיונות העיקריים

חשוב שילדים יבינו שהתוכן שהם מוצאים באינטרנט הוא לא בהכרח נכון או אמין, ושלפעמים הוא נוצר במטרה זדונית לגנוב את המידע או את הזהות שלהם. באמצעות דיוג ותרמיות אחרות באינטרנט, מנסים לגרום למשתמשים בכל הגילאים להגיב להצעות של אנשים שהם לא מכירים או מאנשים שמתחזים למישהו שהם כן מכירים.

### יעדים לתלמידים

- ✓ **להבין** שאם מידע מופיע באינטרנט – זה לא אומר שהוא נכון או אמיתי.
- ✓ **ללמוד** איך פועל דיוג (פישניג), למה זהו סיכון ואיך להימנע מכך.
- ✓ **לקבוע** את האמינות של אתרים ומקורות מידע שונים, ולהיזהר מניסיונות הטעיה, מטענות בלתי מבוססות, מהצעות או פרסים מזויפים ומתרמיות אחרות באינטרנט.

### תקנים רלוונטיים

**תקני ISTE לנשות חינוך ולאנשי חינוך:** 1a, 2c, 3b, 3c, 4b, 5a, 6a, 6d, 7a  
**תקני ISTE לתלמידים 2016:** 1c, 1d, 2b, 2d, 3b, 3d, 7b, 7c  
**תקני למידה של AASL:** I.b.1, 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.d.1, II.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, IV.b.3, V.a.2, VI.a.1, VI.a.2, VI.a.3

# זהירות, זיופים! אוצר מילים



**בוט:** נקרא גם "צ'אט בוט" או "עוזר וירטואלי". זו תוכנה שפועלת באופן אוטומטי באינטרנט או ברשת כדי לענות על שאלות, לבצע פקודות (כמו לתת מסלול נסיעה לבית של החברים החדשים) או לבצע משימות פשוטות (כמו להשמיע שיר).

**דיוג (פשינג):** מצב שבו מישהו מנסה לרמות אתכם כדי שתשתפו פרטי התחברות או מידע אישי אחר באינטרנט. דיוג מתבצע בדרך כלל באמצעות הודעות אימייל, מודעות או אתרים שנראים דומים לאתרים שבהם אתם כבר משתמשים.

**דיוג (פשינג) ממוקד:** תרמית דיוג שבה התוקף ממקד אליכם בצורה מדויקת יותר, בעזרת נתונים מהמידע האישי שלכם.

**תרמית:** ניסיון זדוני להרוויח כסף או להשיג משהו אחר בעל ערך, על ידי הונאת אנשים.

**מהימן:** מישהו שאפשר לסמוך עליו שיעשה את הדבר הנכון, או את הדבר שצריך לעשות.

**אותנטי:** אמיתי, מקורי או מדויק, לא מזויף או מועתק.

**ניתן לאימות:** משהו שאפשר להוכיח או להראות שהוא אמיתי או נכון.

**מטעה:** מידע שקרי, פעולה או הודעה שנועדו להטעות או לבלבל מישהו.

**מניפולציה:** מישהו ששולט באדם אחר או במצב, או משפיע עליהם, בצורה לא הוגנת, לא ישרה או באמצעות איומים. לחלופין, ייתכן שתוכן שנמצא באינטרנט עבר מניפולציה. למשל, תמונה שנערכה כדי שתניחו הנחה שגויה.

**תרמית:** להטעות מישהו כדי להשיג ממנו דבר בעל ערך.

**חומת אש (Firewall):** תוכנית שמגינה על המחשב מפני רוב התרמיות והטריקים.

**זדוני:** מילים או פעולות מרושעות שנועדו לפגוע. עשוי להתייחס גם לתוכנות מזיקות שנועדו לפגוע במכשיר, בחשבון או במידע אישי של אדם מסוים.

**התחזות ברשת (קאטפשינג):** יצירה של זהות או חשבון מזויפים ברשת חברתית, כדי שאנשים ישתפו את המידע האישי שלהם או כדי שיחשבו שהם מתקשרים עם אדם אמיתי שיש לו חשבון, פרופיל או דף אמיתי.

**פתיון הקלקות (קליקבייט):** תוכן, פוסטים או מודעות מטעים באינטרנט שנועדו למשוך תשומת לב כדי שאנשים ילחצו על קישור או דף אינטרנט. המטרה הסופית היא להגדיל מספר צפיות או תנועה לאתר כדי להרוויח כסף.



# זהירות, זיופים: פעילות 1

## אל תבלעו את הפיתיון!

משחק שבו התלמידים בוחנים הודעות שונות של אימייל וטקסט, ומנסים להחליט אילו מההודעות אמיתיות ואילו מהן נשלחו כתרמיות דיוג.

### יעדים לתלמידים



✓ **ללמוד** על טכניקות שבהן אנשים משתמשים לגניבת זהויות.

✓ **לסקור** דרכים למניעה של גניבת זהות.

✓ **לדעת** שכדאי לדבר עם מבוגר שהם סומכים עליו, אם הם סבורים שנפלו קורבן לגניבת זהות.

✓ **לזהות** את הסימנים של ניסיונות דיוג.

✓ **לשים לב** איך משתפים מידע אישי ועם מי משתפים.

### בואו נדבר



#### מה זה בכלל דיוג?

דיוג מתרחש כשמישהו מנסה לגנוב מידע כמו פרטי ההתחברות או פרטי החשבון שלכם, על ידי התחזות לאדם אחר שאתם סומכים עליו, באימייל, בהודעת טקסט או בתקשורת מקוונת אחרת. נוסף לכך, ייתכן שווירוסים יוחדרו למחשבים שלכם דרך הודעות דיוג באימיילים. גם באמצעות ניסיונות להפנות אתכם אל אתרים לא בטוחים מהודעות אלה, או פתיחה של קבצים מצורפים – הווירוסים עלולים להגיע למחשבים. יש וירוסים שמשתמשים ברשימת אנשי הקשר שלכם כדי לתקוף את החברים או בני המשפחה שלכם באותן התקפות דיוג, או התקפות דיוג מותאמות יותר. בסוגים אחרים של תרמיות, ייתכן שתופיע הודעה שמישהו לא תקין במכשיר שלכם כדי להטעות אתכם ולגרום לכם להוריד תוכנה זדונית או בלתי רצויה. חשוב לזכור: אי אפשר לדעת אם משהו לא תקין במכשיר שלכם באמצעות אתר או מודעה!

יש מתקפות דיוג שברור שהן מזויפות. מתקפות אחרות יכולות להיות מתוחכמות ומשכנעות מאוד – למשל, כשתוקף שולח לכם הודעה שכוללת חלק מהמידע האישי שלכם. זה נקרא "דיוג ממוקד" וקשה מאוד לזהות זאת. התוקף משתמש במידע אישי ולכן נראה כאילו הוא מכיר אתכם.

לפני שלוחצים על קישור או מזינים סיסמה באתר שעדיין לא ביקרתם בו, כדאי לשאול את עצמכם כמה שאלות על האימייל או דף האינטרנט. אלה השאלות שכדאי לשאול:

- האם האתר נראה מקצועי כמו אתרים מהימנים שאתם מכירים, וכולל את הלוגו הרגיל של המוצר או החברה וכן טקסטים ללא שגיאות איות?
- האם כתובת האתר תואמת לשם המוצר או שם החברה שאתם מחפשים ולמידע הקשור אליהם?
- האם יש שגיאות איות?
- האם מופיעים חלונות קופצים שנראים כמו ספאם?
- האם כתובת האתר מתחילה ב-<https://> ומופיע מנעול ירוק קטן מימין לכתובת? (פירוש הדבר הוא שהחיבור מאובטח)
- מה כתוב באותיות הקטנות? (שם בדרך כלל מוסיפים פרטים מוטעים)
- האם באימייל או באתר יש הצעה שנשמעת טובה מדי, למשל הזדמנות להרוויח המון כסף? (בדרך כלל זה טוב מדי מכדי להיות אמיתי)
- האם ההודעה נראית קצת מוזרה? כאילו שמכירים אתכם, אבל אתם לא ממש בטוחים?

## פעילות



### החומרים הדרושים:

- דף עבודה: דוגמאות לדיוג

### תשובות לדף העבודה "דוגמאות לדיוג"

1. **אמיתי.** באימייל מתבקש המשתמש להיכנס לאתר החברה ושם להיכנס לחשבון שלו בעצמו, במקום לספק קישור או לבקש שישלח את הסיסמה שלו באימייל (קישורים עלולים להעביר משתמשים לאתרים זדוניים).
2. **מזויף.** כתובת אתר חשודה ולא מאובטחת
3. **אמיתי.** שימו לב להתחלה <https://> בכתובת האתר.
4. **מזויף.** הצעה חשודה בתמורה לפרטי חשבון בנק
5. **מזויף.** כתובת אתר חשודה ולא מאובטחת

ואם בכל זאת נפלתם קורבן לתרמית? דבר ראשון: אל תיבהלו!

- ספרו מיד להורים, למורה או למבוגר אחר שאתם סומכים עליו. ככל שתמתינו זמן רב יותר, המצב עלול להחמיר.
- כדאי לשנות את הסיסמאות לחשבונות המקוונים שלכם.
- אם נפלתם קורבן לתרמית, הודיעו על כך מיד לחברים ולאנשי הקשר שלכם שעלולים להיות המטרה הבאה.
- אם אפשר, השתמשו בהגדרות כדי לדווח על ההודעה כספאם.

### 1. הקבוצות בוחנות את הדוגמאות

בואו נתחלק לקבוצות, וכל קבוצה תבחן את הדוגמאות האלה של הודעות ואתרים.

### 2. כל אחד בוחר באפשרות

מחליטים לגבי כל דוגמה אם מדובר בדבר "אמיתי" או "מזויף", ומפרטים מתחתיה מדוע.

### 3. חברי הקבוצות דנים באפשרויות שנבחרו

אילו דוגמאות נראות לכם מהימנות ואילו נראות חשודות? האם היו תשובות שהפתיעו אתכם? אם כן, למה?

### 4. דיון נוסף

הנה כמה שאלות נוספות שעליכם לשאול את עצמכם כשמבצעים הערכה של הודעות ואתרים באינטרנט:

- **האם ההודעה נראית בסדר?**  
מה תחושת הבטן שלכם? האם אתם מבחינים בחלקים חשודים? האם היא כוללת הצעה לתקן בעיה שלא ידעתם עליה?
- **האם באימייל יש הצעה לקבל משהו בחינם?**  
דברים שמוצעים בחינם בדרך כלל לא באמת מגיעים בחינם.
- **האם ההודעה כוללת בקשה למידע אישי?**  
יש אתרים שמבקשים מידע אישי כדי שיוכלו לשלוח לכם תרמיות נוספות. לדוגמה, חידונים או "מבחני אישיות" יכולים לאסוף עובדות שיעזרו לנחש את הסיסמה שלכם, או מידע סודי אחר. רוב העסקים האמיתיים לא יבקשו מידע אישי באימייל.
- **האם זו הודעת שרשרת באימייל או ברשת החברתית?**  
אימיילים ופוסטים שמבקשים מכם להעביר אותם הלאה לכל מי שאתם מכירים עלולים לסכן אתכם ואחרים. אל תעבירו אותם אלא אם אתם יודעים בוודאות מה המקור, ובטוחים שניתן להעביר את ההודעה בצורה בטוחה.

• האם ההודעה כוללת "אותיות קטנות"?

בחלק התחתון של רוב המסמכים תמצאו את "האותיות הקטנות". מדובר בטקסט קטנטן, שבדרך כלל מכיל את הפרטים שאתם אמורים לפספס. לדוגמה, יכול להיות שהכותרת העליונה תכריז שזכיתם בטלפון חינוך, אבל באותיות הקטנות תקראו שבעצם אתם צריכים לשלם לחברה 800 ש"ח בחודש. אתם צריכים לחשוש גם במקרים שאין בכלל טקסט באותיות קטנות.

הערה: למטרות התרגיל הזה, הניחו ש-*Internaut mail* הוא שירות אמיתי ומהימן.

**מה למדנו?**

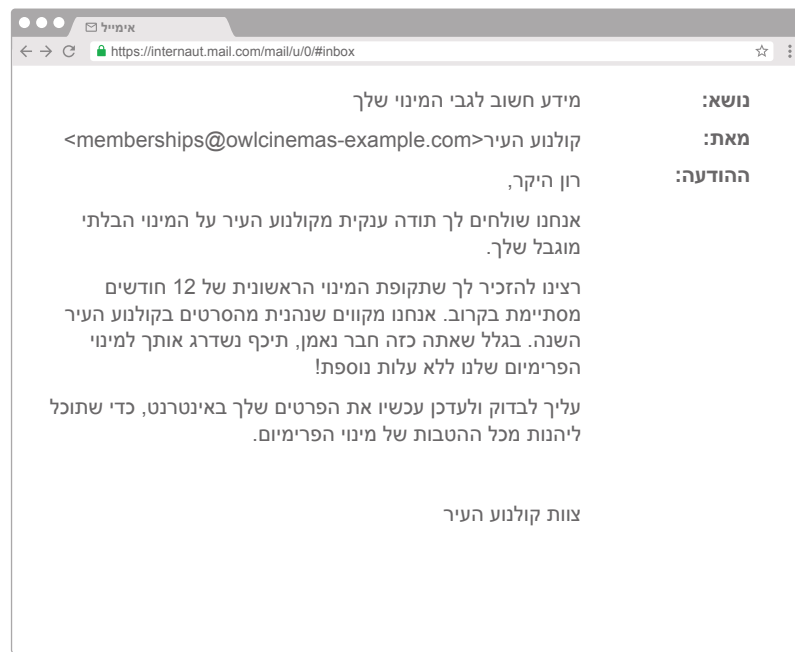
כשאתם גולשים באינטרנט, שימו לב תמיד למצבים של התקפות דיוג באימייל, בהודעות טקסט ובפוסטים. אם בכל זאת נפלתם קורבן לתרמית, כדאי לספר מיד למבוגר שסומכים עליו.

# דף עבודה: פעילות 1

## דוגמאות לדיוג

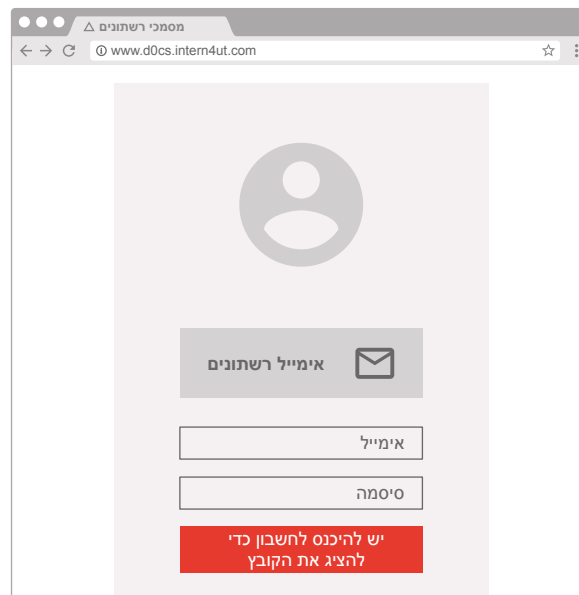
### 1. האם זה אמיתי או מזויף?

מזויף      אמיתי



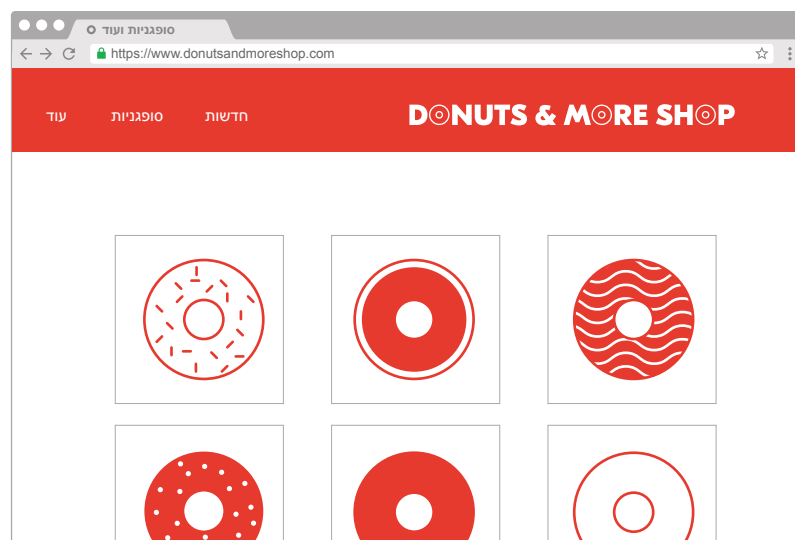
### 2. האם זה אמיתי או מזויף?

מזויף      אמיתי



### 3. האם זה אמיתי או מזויף?

מזויף      אמיתי



#### 4. האם זה אמיתי או מזויף?

מזויף      אמיתי

אימייל

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

☆

⋮

נושא:

הזדמנות מצוינת, חבר

מאת:

רובין <robin@robin-hood-example.com>

הודעה:

חבר יקר,

שמי רותי ואני מורה מפתח תקווה. אני מלמדת קבוצה ענקית של תלמידים ממשפחות בסיכון, ואני מאמינה שיש לי השפעה משמעותית וטובה על החיים שלהם. לצערי, העירייה גובה ממני יותר מדי ארנונה. כידוע לך, מורים מרוויחים ממש מעט ולא אמורים לשלם כל כך הרבה ארנונה. אני עומדת לרשת סכום כסף עצום (יותר מ-5 מיליון שקל) ואני לא רוצה שבעירייה יידעו על זה.

תמיד היית חבר טוב, ולכן אני רוצה להפקיד את הכסף בחשבון הבנק שלך בינתיים. אני מוכנה לתת לך מיליון שקל כפרס. זו עסקה ממש טובה ומיועדת רק לך, חבר יקר. שלח לי את כל פרטי חשבון הבנק שלך כדי שאוכל להפקיד את הכסף בחשבון שלך.

בברכה,

רותי לוי

#### 5. האם זה אמיתי או מזויף?

מזויף      אמיתי

מינוטשר תנובשח

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

☆

⋮

חשבונות רשתונים

הי, זו באמת את?

נראה שנכנסת לחשבונך ממיקום חדש. אנחנו רוצים לדעת שזו את ולא מישהו שמנסה לפרוץ לחשבון שלך. עלייך להשלים את האימות הקצר הזה. ניתן לקבל מידע נוסף על אמצעי האבטחה הזה.

בחירה של שיטת אימות

☒ אימות מספר הטלפון שלי:

יש להזין מספר טלפון מלא

שירות "אימייל רשתונים" יבדוק אם מספר הטלפון הזה זהה למספר ששמור אצלנו, ולא נשלח לך הודעות.

☐ אימות כתובת האימייל לשחזור חשבון:

יש להזין כתובת אימייל מלאה

שירות "אימייל רשתונים" יבדוק אם מספר הטלפון הזה זהה למספר ששמור אצלנו, ולא נשלח לך הודעות.

המשך

## זהירות, זיופים: פעילות 2 מי זה באמת?

התלמידים מתרגלים התמודדות מול דיג על ידי משחק תפקידים ודיון בתגובות אפשריות להודעות טקסט, פוסטים, בקשות חברות, תמונות ואימיילים חשודים.

### יעדים לתלמידים



- ✓ להבין שייתכן שאנשים באינטרנט אינם מי שהם טוענים.
- ✓ לוודא שהאדם הוא אכן מי שהוא טוען שהוא, לפני שעונים לו.
- ✓ לשאול שאלות או לבקש עזרה ממבוגר אם קשה לדעת מי האדם באמת.

### בואו נדבר



#### איך אפשר לדעת מי זה באמת?

כשאתם מדברים בטלפון עם חברים, אתם מזהים אותם לפי הקול שלהם, למרות שלא רואים אותם. אבל העולם המקוון שונה קצת. לפעמים קשה יותר להיות בטוחים שמישהו הוא באמת מי שהוא אומר. באפליקציות ובמשחקים אנשים לפעמים מתחזים למישהו אחר בתור בדיחה או כדי לפגוע במישהו אחר, או שהם מתחזים לאנשים אחרים כדי לגנוב מידע אישי. כשאתם משתמשים באינטרנט, זרים עלולים לנסות ליצור איתכם קשר. הגישה הבטוחה ביותר היא לא להגיב לכך, או לספר להורה או למבוגר שסומכים עליו שאינכם מכירים את האדם שמנסה ליצור איתכם קשר. אם תחליטו שאפשר להגיב, תחילה כדאי מאוד לראות מה תוכלו לגלות עליו. אפשר לבדוק את הפרופיל שלו, לראות מי החברים שלו או לחפש מידע נוסף כדי לאמת את הזהות שלו.

יש מספר דרכים לאמת את הזהות של אדם באינטרנט. נתחיל בכמה דוגמאות.

#### הערה למורה

תחילה, אולי תרצו לערוך סיעור מוחות בכיתה לגבי השאלה "איך לאמת זהות של אדם באינטרנט?" לאחר מכן, תוכלו להמשיך את השיחה עם השאלות האלה כחומר למחשבה.

#### • האם תמונת הפרופיל נראית חשודה?

האם תמונת הפרופיל מטושטשת או לא ברורה? או שאין בכלל תמונה, רק ביטמוג'י או פנים של דמות מצוירת? בעזרת תמונות באיכות גרועה, ביטמוג'י, תמונות של חיות מחמד וכו', קל לאנשים להסתיר את זהותם ברשתות חברתיות. נוכלים רבים גם גונבים תמונות מאדם אמיתי כדי להגדיר פרופיל מזויף ולהתחזות לאדם הזה. האם תוכלו למצוא עוד תמונות של האדם באותו שם?

#### • האם שם המשתמש שלו כולל את שמו האמיתי?

האם שם התצוגה שלו תואם לשם אמיתי ברשת חברתית, למשל? (לדוגמה, כתובת דף הפרופיל של עדי דוד היא [SocialMedia.com/Adidavid](https://www.SocialMedia.com/Adidavid)).

#### • האם הוא כתב על עצמו פרטים אישיים בפרופיל?

אם כן, האם נראה שאדם אמיתי כתב אותם? הרבה פעמים אין הרבה מידע אישי בחלק 'מי אני' בחשבונות מזויפים, ולפעמים מי שיוצר אותם מעתיק פרטים או אוסף אותם באקראי כדי ליצור פרופיל מזויף. האם ניתן לאמת את הפרטים האישיים באמצעות חיפוש?

• כמה זמן החשבון פעיל? האם הפעילות המוצגת תואמת לציפיות שלכם?

האם הפרופיל חדש או שכבר יש בו פעילות רבה? האם יש לכם חברים משותפים, כמו שהייתם מצפים? בדרך כלל, בחשבונות מזויפים אין הרבה תוכן ואין סימנים לכך שאנשים מפרסמים שם, מגיבים או יוצרים קשר.

## פעילות



### החומרים הדרושים:

- עותק של דף העבודה "מי זה באמת?" גזור לרצועות, כשבכל רצועה מופיע תרחיש אחד
- קערה או כלי אחר שבהם יונחו הרצועות (כל קבוצת תלמידים תבחר רצועה אחת מתוכן)
- דף עזר בנושא דיג

### 1. קבוצות סוקרות תרחישים

עכשיו נתחלק לקבוצות. כל קבוצה תבחר תרחיש, ותדון באופן שבו כדאי להגיב למצב שמתואר בו.

### 2. הקבוצות עורכות משחקי תפקידים לפי התרחישים

כל קבוצה תציג במשחק את התרחיש שקיבלה: תלמיד אחד יהיה המספר, תלמיד שני יציג את "ההודעה" ותלמיד שלישי יגיב. תלמיד רביעי יכול להסביר את הסיבות לתגובה שבחרתם בה.

### 3. דיון כיתתי בבחירות של הקבוצות

לסיום, נשתמש בדף העזר הזה כדי לדון בבחירות של כל אחת מהקבוצות. אתם מוזמנים לכתוב הודעות נוספות ומאתגרות יותר. לאחר שתכתבו אותן, החברים בכל קבוצה ישתפו את ההודעות עם הקבוצות האחרות.

## מה למדנו?

אתם קובעים עם מי אתם מדברים באינטרנט. ודאו שהאנשים שאיתם אתם יוצרים קשר הם באמת מי שהם טוענים שהם!

## דף עבודה: פעילות 2

# מי זה באמת?

### תרחיש 1

אדם זר שולח אליכם בקשת חברות באינטרנט. "היי! נראה לי שאתה בן אדם כיפי. בטח נוכל לבלות יחד. תוסיף אותי לרשימת החברים שלך? —ירון"

### תרחיש 2

אתם מקבלים הודעת טקסט בסלולרי שלכם ממישהו שאתם לא מזהים.  
"היי, זה אורי! זוכרת אותי מהחופש הגדול?"

### תרחיש 3

אתם מקבלים הודעה ממישהו שאתם לא עוקבים אחריו. "היי! אני מתה על הפוסטים שלך, אתה כזה מצחיק! אולי תיתן לי את מספר הטלפון שלך כדי שנוכל לדבר?"

### תרחיש 4

אתם מקבלים הודעת צ'אט ממישהו שאתם לא מכירים. "ראיתי אותך בשיעור מתמטיקה היום. אתה חמוד! מה הכתובת שלך? אני יכולה לבוא אליך אחרי הצהריים."

### תרחיש 5

אתם מקבלים הודעה באינטרנט. "היי, פגשתי עכשיו את החברה שלך עמית! היא סיפרה לי עלייך, ואני אשמח לפגוש אותך. מה הכתובת שלך?"



## דף עזר בנושא דיוג: פעילות 2

# מי זה באמת?

לפניכם חמישה תרחישים של הודעות, שכל אחד עשוי לקבל באינטרנט או בטלפון. לכל תרחיש יש רשימה של דרכי תגובה, חלקן מעולות וחלקן לא ממש. קראו והחליטו אם הן נראות לכם. אולי תוכלו לחשוב על תגובות נוספות. אם אחד התרחישים האלה יקרה לכם ולא תהיו בטוחים מה לעשות, התגובה הקלה ביותר היא לא להגיב. תמיד אפשר להתעלם מהשולח או לחסום אותו, ותמיד כדאי לדבר על זה עם הורה או מורה.

### תרחיש 1

אתם מקבלים את ההודעה הזו ממישהו שאינכם מזהים: "היי! נראה לי שאתה בן אדם כיפי. בטח נוכל לבלות יחד. תוסיף אותי לרשימת החברים שלך? — ירון" מה לעשות?

• **להתעלם מירון.** אם אתם לא מכירים אותו, אתם יכולים פשוט להחליט לא לדבר איתו, וזהו.

• **"היי ירון, אנחנו מכירים?"** אם לא בטוחים, קודם שואלים.

• **לחסום את ירון.** אם בדקתם מי זה והחלטתם לחסום אותו, לא תקבלו ממנו הודעות נוספות. ברוב הפלטפורמות של הרשתות החברתיות, הוא אפילו לא יידע שחסמתם אותו.

• **לבדוק את הפרופיל של ירון.** צריך להיזהר – קל ליצור פרופיל מזויף! אפשר לבדוק את רשימת החברים שלו ולראות עם מי הוא יוצר קשר. גם מעגל החברים שלו יכול לעזור לכם לגלות אם הוא אמיתי או לא, במיוחד אם אתם לא מכירים אף אחד מחבריו! אם אין הרבה פעילות בדף שלו, זה רמז נוסף לכך שהוא לא אמיתי.

• **להוסיף את ירון לרשימת החברים שלכם.** אם הוא נראה בסדר. לא מומלץ, אלא אם וידאתם מיהו ובדקתם את העניין עם מבוגר שאתם סומכים עליו.

• **לתת לו פרטים אישיים.** אף פעם אל תמסרו מידע אישי לאנשים שאתם לא מכירים.

### תרחיש 2

אתם מקבלים הודעת טקסט בסלולרי שלכם ממישהו שאתם לא מזהים. "היי, זה אורי! זוכרת אותי מהחופש הגדול?" מה לעשות?

• **לחסום את אורי.** אם אתם מכירים אותו, לא נעים לחסום. אבל אם אתם בטוחים שלא פגשתם מישהו בשם אורי בחופש הגדול, או שהוא שולח לכם יותר מדי הודעות ומשתף יותר מדי פרטים על עצמו, אפשר בהחלט לחסום אותו.

• **להתעלם מאורי.** אם אתם לא מכירים אותו, אפשר פשוט לא להגיב.

• **"היי אורי, אנחנו מכירים?"** זו אפשרות בטוחה אם אתם לא בטוחים שאתם מכירים אותו, ורוצים לגלות מידע נוסף כדי לדעת מי זה. אבל אל תגלו לאורי איפה הייתם בחופש הגדול!

• **"אני לא זוכר אותך, אבל אפשר להיפגש מתישהו".** ממש לא רעיון טוב. אף פעם אל תציעו להיפגש עם מישהו שאתם לא מכירים.

### תרחיש 3

אתם מקבלים הודעה מ-soccergirl12, ואתם לא עוקבים אחריה. "היי! אני מתה על הפוסטים שלך, אתה כזה מצחיק! אולי תיתן לי את מספר הטלפון שלך כדי שנוכל לדבר?" מה לעשות?

• **להתעלם מ-soccergirl12.** אתם לא חייבים להגיב אם אתם לא רוצים.

• **לחסום את soccergirl12.** אם האדם הזה נראה לכם חשוד ותחסמו אותו, לא תשמעו ממנו יותר - אלא אם הוא ייצור פרופיל מזויף חדש וינסה לפנות אליכם כדמות אחרת.

• **"היי, אנחנו מכירים?"** אם אתם לא בטוחים, תשאלו שאלות לפני שתמסרו פרטים אישיים כמו מספר טלפון.

• **"אוקיי, המספר שלי הוא..."** לא! גם אם וידאתם מי האדם הזה, לא מומלץ למסור מידע אישי במדיה חברתית. כדאי למצוא דרך אחרת ליצור קשר, דרך הורים, מורים או אדם מהימן אחר.

### תרחיש 4

אתם מקבלים הודעת צ'אט ממישהו שאתם לא מכירים. "ראיתי אותך בשיעור מתמטיקה היום. אתה חמוד! מה הכתובת שלך? אני יכולה לבוא אליך אחרי הצהריים." מה לעשות?

• **להתעלם.** זו כנראה בחירה נכונה.

• **לחסום את האדם הזה.** אם יש לכם הרגשה רעה לגבי מישהו, אל תהססו.

• **"מי זה?"** לא מומלץ. אם ההודעה נשמעת חשודה, לא כדאי להשיב לה, אלא לחסום את השולח.

• **"זאת את, שחר? גם את ממש חמודה! אני גר ברחוב המעגל 50."** זה לא רעיון טוב, גם אם אתם חושבים שאתם יודעים מי שלחה את ההודעה. לפני שתמסרו למישהו חדש את הכתובת שלכם או מידע אישי אחר, חשוב לבדוק את האדם הזה, גם אם אתם חושבים שאתם מכירים אותו. אף פעם אל תיפגשו פנים-אל-פנים עם אדם שאתם מכירים רק מתוך תקשורת באינטרנט ללא אישור ההורים.

קיבלתם את ההודעה הזו: "היי, פגשתי עכשיו את החברה שלך עמית! היא סיפרה לי עלייך ואשמח לפגוש אותך. מה הכתובת שלך?" מה לעשות?

• **להתעלם.** אם אתם לא מכירים את האדם הזה אבל יש לכם חברה בשם עמית, האפשרות הטובה ביותר היא לבדוק קודם עם עמית לפני שתשיבו להודעה הזו.

• **לחסום.** אם אתם לא מכירים את האדם הזה ואין לכם חברה בשם עמית, כדאי להשתמש בהגדרות שלכם כדי לחסום אותו ולמנוע ממנו לשלוח לכם הודעות נוספות.

• **"מי זה?"** לא ממש רעיון טוב. אם אתם לא מכירים את האדם הזה, עדיף לא להשיב לו, לפחות עד שתבררו את הנושא עם עמית.

כיום יש אינטראקציה הולכת וגוברת בין תלמידים לבין "קולות" שבוקעים ממכשירים, מאפליקציות ומאתרים – בעיקר בבית, אבל בהדרגה גם בבית הספר. לפעמים הם נקראים "צ'אט בוט", עוזר וירטואלי, ובדרך כלל פשוט "בוט". זו פעילות פשוטה של שאלות ותשובות, ומטרתה שכל תלמידי הכיתה יחשבו וידונו יחד בנושא אינטראקציה עם בוטים.

הערה: חשוב לנהל דיון פתוח. פעילות זו נועדה לפתח חשיבה ביקורתית, ולא להציג מסקנות כלשהן.

### יעדים לתלמידים



- ✓ **ללמוד** על הטכנולוגיה האינטראקטיבית הזו שצצה בעוד ועוד מקומות בחייהם של התלמידים.
- ✓ **לזהות** חוויות שימוש בבוטים מסוגים שונים.
- ✓ **לנתח** את ההשפעה שעשויה להיות לטכנולוגיות אלה על חיי היומיום – הן השפעה חיובית והן שלילית.

### בואו נדבר



יותר ויותר אנשים משתמשים כיום בבוטים. האם שמעתם את המילה הזו כבר? יש אנשים שקוראים להם "צ'אט בוטים" או "עוזרים וירטואליים". הם משמשים למיליון פעולות: לשחק משחקים, לבדוק מה מזג האוויר, לענות על שאלות, לקבל מסלולי נסיעה, להודיע לכם שהגיע הזמן וכו'. לפעמים יש להם שם אנושי, ולפעמים השם שלהם פשוט מתאר את פעולתם. למשל, "כלב ליום" הוא בוט ששולח תמונה של כלב בכל יום. בוטים יכולים לפעול בניידים, באינטרנט, במכונות או שהם פשוט מכשירים מיוחדים שיש לאנשים בחדרים שונים בבית. בואו נדבר על החוויות שהיו לתלמידי הכיתה עם בוטים, ונתחיל בתהליך החשיבה על הנושא. הנה כמה שאלות שכדאי להעלות:

- האם אתם יודעים מהו בוט?
- כמה מכם דיברו עם בוט? באיזה סוג מכשיר?
- מי רוצה לספר לנו על החוויה שלו?
- לאילו פעולות, לדעתכם, הבוטים הכי מתאימים (דוגמאות שיעזרו להם לענות: לבקש תחזית מזג-אוויר, לשמוע חדשות, לשחק משחק, לבקש מידע)?
- בוטים משתמשים בטכנולוגיית AI, או בינה מלאכותית. באמצעות AI, המכשיר לומד על מה שאתם שואלים אותו כדי שהוא יוכל לעזור לכם בצורה טובה יותר. לשם כך, לעתים בוטים "זוכרים", או מקליטים, את מה שאתם מבקשים ואומרים. בעקבות זאת, האם אתם חושבים על מה שכדאי לומר לבוט? אם כן, מה תגידו לו ואיזה מידע לא תרצו לגלות?
- אתם חושבים שזה דומה לשיחה עם אדם? מה הדברים הדומים ומה שונה בכך?
- איך אנשים שאתם מכירים מתייחסים לבוטים או מדברים אליהם?
- איך תדברו אליהם? האם תהיו מנומסים או שתצעקו עליהם לפעמים?
- האם זה בסדר לצעוק על בוטים? למה כן ולמה לא? (האם זה כמו להתאמן על סוג מסוים של אינטראקציה?)
- לפעמים, ילדים קטנים מאוד חושבים שבוטים הם בני-אדם. מה הייתם אומרים לאחות, אח או בן דוד צעירים כדי שיבינו עם מי הם מדברים?

- אם בוטים יכולים ללמוד מאנשים, תוכלו לחשוב על משהו שלא כדאי לומר כי לא תרצו שהבוט יידע אותו? (רמז: אפשר להיזכר בפעילויות שבקטע "חושבים לפני שמתפנים", ולראות איך הן קשורות לנושא שלנו)
- האם ניתן לסווג מידע כ"טוב או רע", או כ"אמיתי או מזויף"? איך אפשר לנסות לענות על השאלות האלה?

## פעילות



לאחר הדיון, כל תלמידי הכיתה או בקבוצות עם מכשירים נפרדים, מחפשים תמונות של בוטים ומידע עליהם (כולל סיקור חדשותי). מונחי החיפוש יכולים לכלול "בוטים", "צ'אט בוטים", "עוזרים דיגיטליים", או "עוזרים וירטואליים". תלמידי הכיתה מחליטים אם המידע אמין. הם בוחרים מאמר אחד כדי לקחת הביתה, לקרוא עם ההורים שלהם ולכתוב עליו סיכום באורך פיסקה אחת.

## מה למדנו?

חשיבה ביקורתית היא אחד מהכלים הטובים ביותר, שפועלים לטווח הרחוק ועוזרים לנו להשתמש בטכנולוגיה בצורה חיובית. זה כלי שמשתפר בכל פעם שאנחנו משתמשים בו. באמצעות חשיבה ודיון משותפים, אפשר להשתמש בכלי הזה ולשפר אותו בצורה משמעותית ומהנה.

## ממלכת האינטרנט: נהר האמת והשקר

בנהר שחוצה את ממלכת האינטרנט זורם מידע שכולל אמיתות ושקרים. אבל לפעמים קשה להבדיל ביניהם. כדי לחצות את הנהר, עליכם להפעיל שיקול דעת. ואל תיפלו בפח שטומן לכם הדייגן שאורב במים.

יש לפתוח דפדפן אינטרנט במחשב או בנייד שלכם (לדוגמה, בטאבלט) ולהיכנס אל [g.co/RealityRiver](http://g.co/RealityRiver).

### נושאים לדיון



- התלמידים ישחקו ב"נהר האמת והשקר", ובעזרת השאלות הבאות ידונו במה שהם למדו מהמשחק.
- רוב התלמידים מפיקים את מירב התועלת ממשחק עצמאי, אבל התלמידים יכולים גם לשחק בזוגות. זה יכול לעזור במיוחד לתלמידים צעירים.
- תארו מצב שבו הייתם צריכים להחליט אם המידע באינטרנט הוא אמת או שקר. באילו סימנים הבחנתם?
- מהו דייגן? תארו איך הוא מתנהג ואיך הוא משפיע על המשחק.
- האם המשחק ב"נהר האמת והשקר" יגרום לכם לשנות את אופן ההערכה של תוכן ואנשים באינטרנט בעתיד? אם כן, כיצד?
- תארו פעולה אחת שתעשו אחרת בעקבות השיעורים האלה וההתנסות במשחק הזה.
- מה יכולים להיות הרמזים לכך שיש משהו מוזר או מפחיד במצב מסוים באינטרנט?
- איך אתם מרגישים כשאתם נתקלים במצב מוזר באינטרנט?
- אם אתם לא בטוחים אם תוכן כלשהו אמיתי, מה צריך לעשות?

**הערות**





# שומרים על הסודות שלנו

## מידע מעשי לגבי פרטיות ואבטחה

### סקירה כללית של השיעור

פעילות 1: איך יוצרים סיסמה מעולה  
פעילות 2: שומרים על פרטיות  
פעילות 3: ממלכת האינטרנט: מבצר הסיסמאות

### הרעיונות העיקריים

לפעמים, לבעיות הקשורות לפרטיות ולאבטחה באינטרנט אין פתרונות שברור שהם נכונים או שגויים. כדי להגן על המידע הפרטי והאישי שלכם – כל מה שמייצג אתכם, צריך לשאול את השאלות הנכונות ולמצוא תשובות מושכלות משלכם.

### יעדים לתלמידים

- ✓ ללמוד למה פרטיות חשובה ואיך היא קשורה לאבטחה מקוונת.
- ✓ לתרגל יצירת סיסמאות חזקות.
- ✓ לסקור את הכלים וההגדרות שמגינים מפני האקרים ואיומים אחרים.

### תקנים רלוונטיים

תקני ISTE לנשות חינוך ולאנשי חינוך: 1a, 2c, 3b, 3c, 3b, 4b, 6a, 6d, 7a  
תקני ISTE לתלמידים 2016: 1c, 1d, 2b, 2d, 3d, a6  
תקני למידה של AASL: I.b.2, I.c.1, I.c.3, II.c.1, III.a.2, III.b.1, III.c.1, III.d.1, III.d.2, IV.b.3, V.d.3, VI.a.1, VI.d.1

# שומרים על הסודות שלנו

## אוצר מילים



**פרטיות:** הגנה על הנתונים ועל המידע האישי של אנשים (נקרא גם "מידע רגיש")

**אבטחה:** הגנה על מכשירים של אנשים ועל התוכנה שמותקנת בהם

**אימות דו-שלבי (נקרא גם אימות דו-גורמי):** תהליך אבטחה שכולל שני שלבים, או שני "גורמים", הנדרשים כדי להתחבר לשירות מסוים. למשל, סיסמה וקוד חד-פעמי. לדוגמה, ייתכן שתידרשו להזין את הסיסמה שלכם ולאחר מכן קוד שנשלח אל מספר הטלפון שלכם, או קוד מאפליקציה מסוימת.

**סיסמה או קוד גישה:** צירוף סודי המשמש לגישה למשהו. יש סוגים שונים של סיסמאות. לדוגמה, ייתכן שיהיה לכם קוד בן 4 ספרות לנעילת הטלפון, וסיסמה מורכבת הרבה יותר לחשבון האימייל. בעיקרון, מומלץ ליצור סיסמאות ארוכות ומורכבות ככל שניתן, אבל שעדיין תוכלו לזכור אותן.

**הצפנה:** תהליך המרה של מידע או של נתונים לקוד כדי שלא ניתן יהיה לקרוא אותם ולגשת אליהם

**מורכבות:** המטרה של יצירת סיסמה מאובטחת. לדוגמה, סיסמה מורכבת כוללת שילוב של מספרים, תווים מיוחדים (כמו \$ או &) וכן אותיות גדולות וקטנות.

**האקר:** אדם שמשתמש במחשבים כדי לקבל גישה בלתי מורשית למכשירים ולנתונים של אנשים אחרים ושל ארגונים

# שומרים על הסודות שלנו: פעילות 1

## איך יוצרים סיסמה מעולה

התלמידים לומדים איך ליצור סיסמה חזקה – ומקפידים לשמור עליה בסוד לאחר יצירתה.

### יעדים לתלמידים



- ✓ להבין שחשוב לא לשתף סיסמאות אף פעם, פרט לשיתוף עם הורים או אפטרופסים
- ✓ להבין למה חשוב שיהיו נעילות מסכים שמגינות על מכשירים
- ✓ לדעת איך ליצור סיסמאות שקשה לנחש וקל לזכור
- ✓ לבחור את האבטחה הנכונה להגדרות ההתחברות שלהם, כולל אימות דו-גורמי.

### בואו נדבר



#### עדיף להגן על המידע מאשר להצטער שלא עשינו זאת

טכנולוגיה דיגיטלית מאפשרת לנו לתקשר בקלות עם חברים, תלמידים אחרים בכיתה, מורים ובני משפחה. אנחנו יכולים לתקשר עם העולם בכל כך הרבה דרכים: באמצעות אימייל, הודעות טקסט והודעות מיידיות; במילים, בתמונות ובסרטונים; באמצעות טלפונים, טאבלטים ומחשבים ניידים. (איך אתם מתקשרים עם החברים שלכם?)

עם זאת, אותם הכלים שמקלים עלינו לשתף את המידע גם מקלים על האקרים ונוכלים לגנוב את המידע הזה ולהשתמש בו כדי לפגוע במכשירים, בקשרים ובמוניטין שלנו.

כדי להגן על עצמנו, על המידע ועל המכשירים שלנו, אנחנו צריכים לבצע פעולות פשוטות וחכמות. למשל, להשתמש בנעילות מסכים בטלפונים, להיזהר כשאנחנו שומרים מידע אישי במכשירים לא נעולים שאנחנו עלולים לאבד או שעשויים להיגנב, ומעל לכל, ליצור סיסמאות חזקות. כדי שלא תשכחו את הסיסמאות, כדאי לבקש מההורים לרשום אותן אצלם.

- מי יכול לנחש מהן שתי הסיסמאות הנפוצות ביותר? (תשובה: "1 2 3 4 5 6" ו-"password")
- בואו נחשוב על עוד כמה סיסמאות גרועות, והסיבה לכך שהן גרועות. (דוגמאות: השם המלא שלכם, מספר הטלפון שלכם, המילה "chocolate")

מי חושב שהסיסמאות האלה טובות? ;

### פעילות



הנה רעיון ליצירת סיסמה מאובטחת במיוחד:

- חושבים על משפט משעשע באנגלית שיהיה לכם קל לזכור. זה יכול להיות שורה מהשיר האהוב עליכם, שם ספר, משפט קליט מסרט וכו'.
- בוחרים את האות הראשונה או שתי האותיות הראשונות של כל מילה במשפט.
- משנים חלק מהאותיות למספרים או לסמלים.
- כותבים חלק מהאותיות כאותיות גדולות וחלק כקטנות.
- כדי לתרגל את המיומנויות החדשות שלנו, נשחק במשחק הסיסמה.

#### 1. יוצרים סיסמאות

נתחלק לזוגות. כל זוג צריך ליצור סיסמה תוך 60 שניות (אתגר: התלמידים משתפים רמזים עם הכיתה, כדי לראות כמה נתוני הקשר נדרשים לכיתה כדי לנחש במדויק).

#### החומרים הדרושים:

- מכשירים עם חיבור לאינטרנט
- תלמידים או לקבוצות של תלמידים
- לוח או מסך הקרנה
- דף העבודה "הנחיות ליצירת סיסמאות חזקות"

## 2. משווים סיסמאות

בכל פעם, שני זוגות יכתבו את הסיסמה שלהם על הלוח.

## 3. מצביעים!

לגבי כל זוג סיסמאות, כולנו נצביע לסיסמה החזקה ביותר ונבחן מדוע היא חזקה יותר.

## מה למדנו?

## הנחיות ליצירת סיסמאות חזקות

חשוב ליצור סיסמאות חזקות וכיף ליצור אותן.

לפניכם כמה טיפים ליצירת סיסמאות כדי להגן על המידע שלכם.

**סיסמאות חזקות** מבוססות על ביטוי או משפט תיאורי שקל לכם לזכור וקשה לאדם אחר לנחש. לדוגמה, האותיות הראשונות בכל מילה בשם של ספר או שיר שאוהבים, האותיות הראשונות בכל מילה במשפט שמספר על פעולה שעשיתם. כמו כן, הסיסמאות צריכות לכלול שילוב של אותיות, מספרים וסמלים. למשל, מהמשפט "I went to Western Elementary School for grade 3" אפשר ליצור סיסמה כזו: lw2We\$4g3.

**סיסמאות סבירות** הן סיסמאות חזקות שלא קל לנחש אותן באמצעות תוכנה זדונית, אבל מישהו שמכיר אתכם כן עשוי לנחש אותן (לדוגמה, IwenttoWestern).

**סיסמאות חלשות** כוללות בדרך כלל מידע אישי, קל לפצח אותן, ומישהו שמכיר אתכם יכול לנחש אותן (כמו IloveBuddy או Ilikechocolate).

## מה לעשות

- להשתמש בסיסמה שונה לכל אחד מהחשבונות החשובים שלכם.
- להשתמש בשמונה תווים לפחות. כמה שיותר ארוך, יותר טוב (כל עוד אתם זוכרים את הסיסמה!).
- להשתמש בשילוב של אותיות (רישיות וקטנות), מספרים וסימנים.
- חשוב שתוכלו לזכור את הסיסמאות כדי שלא תצטרכו לכתוב אותן, כי זה עלול להיות מסוכן.
- יש לשנות את הסיסמה מיד אם אתם יודעים או סבורים שגילה אותה מישהו שאינו מבוגר שאתם סומכים עליו.
- להשתמש תמיד בנעילות מסכים חזקות במכשירים שלכם. כדאי להגדיר נעילה אוטומטית במכשיר, למקרה שהוא ייפול לידיים הלא נכונות.
- אפשר להשתמש במנהל סיסמאות כדי לזכור את כל הסיסמאות, למשל, מנהל סיסמאות שמובנה בדפדפן. כך תוכלו להשתמש בסיסמה ייחודית לכל חשבון ולא תצטרכו לזכור את כולן.

## מה לא לעשות

- לא להשתמש במידע אישי (שם, כתובת, אימייל, מספר טלפון, מספר זהות, שם נעורים של האם, תאריכי לידה וכו') או במילים נפוצות בסיסמה שלכם
- לא להשתמש בסיסמה שקל לנחש, כמו הכינוי שלכם, שם בית הספר שלכם, קבוצת הכדורגל האהובה עליכם, מחרוזת מספרים (כמו 123456) וכו' ואל תשתמשו בשום אופן במילה password!
- לא לשתף את הסיסמה שלכם עם אף אחד פרט להורים או לאפוטרופוס שלכם.
- לא לכתוב אף פעם סיסמאות במקום גלוי.

## שומרים על הסודות שלנו: פעילות 2

# שומרים על פרטיות

המורה משתמשת במכשיר בית ספרי כדי להדגים לאן צריך לגשת ומה צריך לחפש כשקובעים את הגדרות הפרטיות.

### יעדים לתלמידים



- ✓ **להתאים אישית** את הגדרות הפרטיות של השירותים המקוונים שבהם התלמידים משתמשים
- ✓ **לקבל החלטות** לגבי שיתוף מידע באתרים ובשירותים שבהם התלמידים משתמשים
- ✓ **להבין** מה המשמעות של אימות דו-שלבי ושל אימות דו-גורמי ומתי כדאי להשתמש בהם.

### בואו נדבר



#### פרטיות = אבטחה

פרטיות ואבטחה באינטרנט הולכות יד ביד. רוב האפליקציות והתוכנות מציעות דרכים שמאפשרות לקבוע איזה מידע נשתף ואיך נשתף אותו.

כשאתם משתמשים באפליקציה או באתר, חפשו אפשרות כמו 'החשבון שלי' או 'הגדרות'. שם תמצאו את הגדרות הפרטיות והאבטחה שיאפשרו לכם לקבוע:

- איזה מידע יופיע בפרופיל שלכם
- מי יוכל לראות את הפוסטים, התמונות, הסרטונים או תוכן אחר שתשתפו

עליכם לדעת להשתמש בהגדרות האלה כדי להגן על הפרטיות שלכם ולזכור לעדכן אותן בעת הצורך. הן יעזרו לכם לנהל את הפרטיות, האבטחה והבטיחות שלכם. חשוב שההורים או האפוטרופוס שלכם תמיד יעזרו לכם לקבל החלטות כאלה.

#### סוקרים את האפשרויות

- המכשיר הבית ספרי מחובר למסך ההקרנה. בואו נעבור לדף ההגדרות של האפליקציה הזו, שם אפשר לראות את האפשרויות. עזרו לי (מעודדים את התלמידים כדי שיעזרו)...
- לשנות את הסיסמה
  - לעבור על הגדרות השיתוף, המיקום ועוד הגדרות, ולהחליט אילו הגדרות הכי מתאימות לכם
  - לקבל התראות אם מישהו מנסה להתחבר לחשבון שלכם ממכשיר לא מוכר
  - להגדיר את חשיפת הפרופיל המקוון שלכם – כולל תמונות וסרטונים - רק למעגלים של בני משפחה וחברים שתבחרו בהם
  - להפעיל אימות דו-שלבי או אימות דו-גורמי
  - להגדיר פרטי שחזור למקרה שלא תוכלו להיכנס לחשבון.

מומלץ לדבר עם ההורה או האפוטרופוס שלכם על ההגדרות של הפרטיות והאבטחה שמתאימות לכם. אבל צריך לזכור שהגדרת האבטחה החשובה ביותר מתחילה בראש שלכם – אתם מקבלים את ההחלטות החשובות בנוגע לכמות המידע האישי שאתם רוצים לשתף, מתי לשתף ועם מי לשתף.

### פעילות



#### החומרים הדרושים:

- מחשב בית-ספרי אחד שמחובר למקרן, ובאמצעותו ניתן להציג בכיתה חשבון לדוגמה (למשל, חשבון אימייל זמני או חשבון זמני באתר כלשהו)

### מה למדנו?

השלב הראשון והחשוב הוא לבחור סיסמה חזקה וייחודית לכל אחד מהחשבונות החשובים שלכם. כמו כן, צריך לזכור את הסיסמאות ולשמור עליהן בסוד.

## שומרים על הסודות שלנו: פעילות 3

# ממלכת האינטרנט: מבצר הסיסמאות

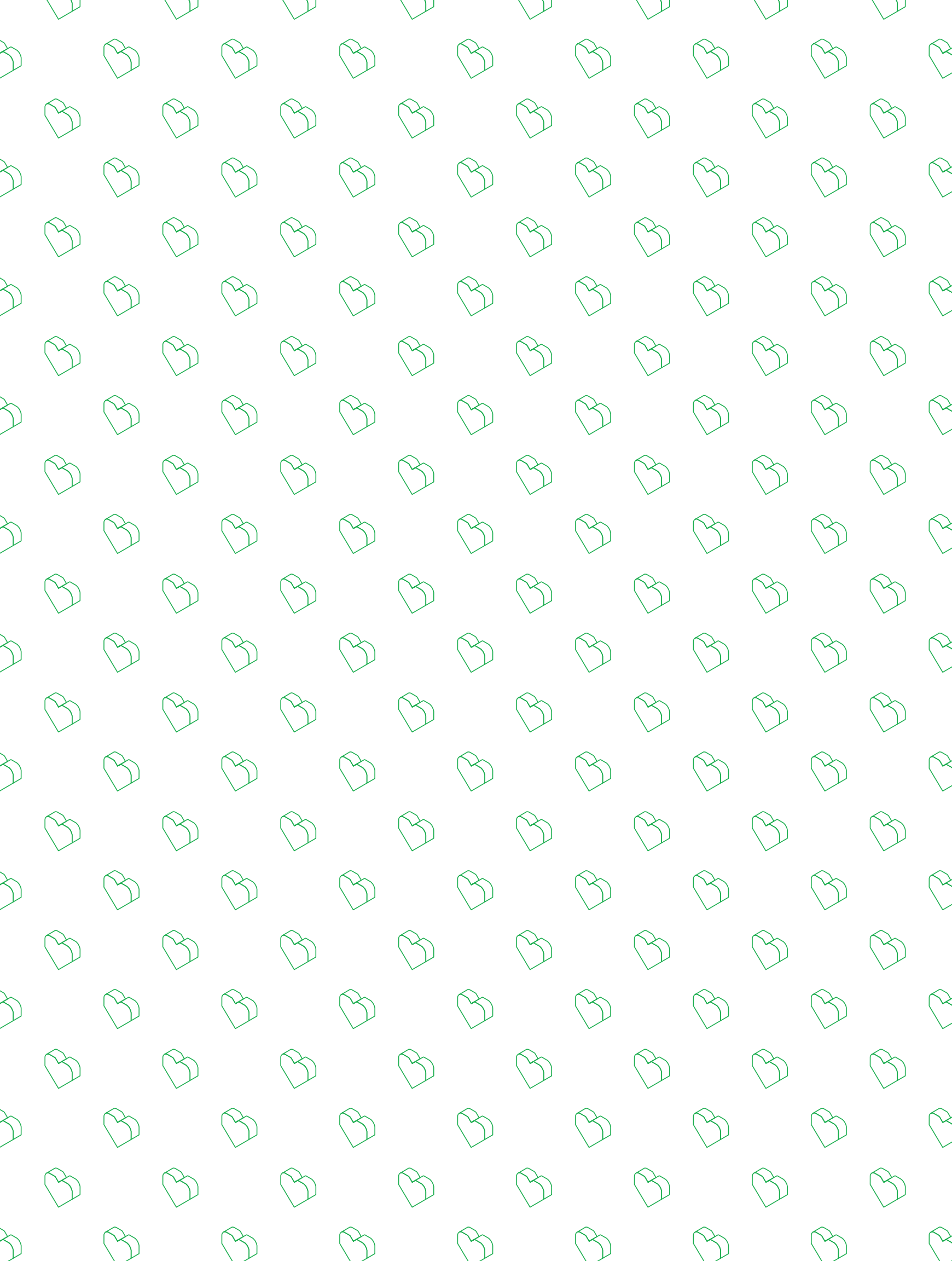
הצילו! מבצר הסיסמאות לא נעול, והמידע של הרשתון (כמו פרטי אנשי קשר והודעות פרטיות) בסכנה. עליכם להשיג את ההאקר ולבנות מבצר עם סיסמאות חזקות כדי לשמור על הסודות שלכם לנצח.

יש לפתוח דפדפן אינטרנט במחשב או בנייד שלכם (לדוגמה, בטאבלט) ולהיכנס אל [g.co/TowerOfTreasure](http://g.co/TowerOfTreasure).

### נושאים לדיון



- התלמידים ישחקו ב"מבצר הסיסמאות", ובעזרת השאלות הבאות ידונו במה שהם למדו מהמשחק. רוב התלמידים מפיקים את מירב התועלת ממשחק עצמאי, אבל התלמידים יכולים גם לשחק בזוגות. זה יכול לעזור במיוחד לתלמידים צעירים.
- מה כוללת סיסמה חזקה במיוחד?
  - מתי חשוב ליצור סיסמאות חזקות בחיים האמיתיים? אילו טיפים למדתם לגבי יצירת סיסמאות חזקות?
  - מה זה האקר? תארו את התנהגות הדמות הזו ואיך היא משפיעה על המשחק.
  - בעקבות המשחק ב"מבצר הסיסמאות", האם בכוונתכם לשנות את אופן ההגנה על המידע שלכם בעתיד?
  - תארו פעולה אחת שתעשו אחרת בעקבות השיעורים האלה וההתנסות במשחק הזה.
  - כתרגול, צרו שלוש סיסמאות שעומדות בקריטריונים לסיסמאות "חזקות במיוחד".
  - תנו דוגמאות למידע רגיש שצריך להגן עליו.





# מגניב להיות אדיב

## כוחה של חוביות באינטרנט

### סקירה כללית של השיעור

- פעילות 1: מעמדת הצופים מהצד לעמדת הצופים המתעורבים
- פעילות 2: אפשרויות לצופים שמתעורבים
- פעילות 3: ... אבל תגידו את זה בצורה יפה!
- פעילות 4: שימו לב לטון שלכם
- פעילות 5: להתנהג בהתאם
- פעילות 6: ממלכת האינטרנט: ממלכת האדיבות

### הרעיונות העיקריים

העולם הדיגיטלי יוצר הזדמנויות ואתגרים חדשים לאינטראקציה חברתית, לילדים ולמבוגרים. קשה יותר לקלוט רמזים חברתיים באינטרנט, החיבור הבלתי פוסק עשוי להוביל להרגשת נוחות וגם לחרדה, אנונימיות יכולה להוביל להתאהבויות ולמחמאות אבל גם לפגיעה עצמית ופגיעה באחרים.

זה מצב מורכב אבל אנחנו יודעים שבעזרת האינטרנט, ניתן להגביר ולהפיץ אדיבות, ולא רק שליליות. חשוב ללמוד להפגין אדיבות ואמפתיה, ואיך להגיב לשליליות ולהטרדה. רק כך נוכל לבנות קשרים בריאים ולהפחית רגשות של בידוד חברתי, שיכולים לפעמים להוביל לבריונות, לדיכאון, לקשיים בלימודים ולבעיות אחרות.

מחקרים מראים שלא מספיק לומר לילדים לא להתנהג בשליליות באינטרנט. מניעה יעילה של בריונות, לעומת זאת, מטפלת בגורמים להתנהגות השלילית. פעילויות אלה מעודדות תלמידים לנהל אינטראקציות חוביות מהתחלה, ומלמדות אותם איך להתמודד עם גישה שלילית כשהם נתקלים בכך.

### יעדים לתלמידים

- ✓ להגדיר מה זאת התנהגות חובית באינטרנט ובמקומות אחרים
- ✓ להוביל באמצעות גישה חובית בתקשורת מקוונת
- ✓ לזהות מצבים שבהם צריך להתייעץ עם מבוגר שסומכים עליו.

### תקנים רלוונטיים

תקני ISTE לנשות חינוך ולאנשי חינוך: 1a, 1c, 2c, 3a, 3b, 3c, 4b, 5a, 5b, 6a, 6b, 6d, 7a  
 תקני ISTE לתלמידים 2016: 1c, 2b, 3d, 4d, 7a, 7b, 7c  
 תקני למידה של AASL: I.a.1, I.a.2, I.b.1, I.b.2, I.b.3, 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.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

# מגניב להיות אדיב

## אוצר מילים



**בריונות:** התנהגות מרושעת ומכוונת, שבדרך כלל חוזרת על עצמה. לרוב, לקורבן קשה להגן על עצמו.

**בריונות ברשת:** בריונות שמתרחשת באינטרנט או באמצעות מכשירים דיגיטליים

**הטרדה:** מונח כללי יותר מבריונות. הטרדה עשויה להתרחש בדרכים שונות – הצקה, איום, השפלה וכו' – ועשויה להתרחש גם באינטרנט

**קונפליקט:** ויכוח או חוסר הסכמה שלא בהכרח חוזרים על עצמם

**הצד התוקף:** האדם שמטריד או שמשמש בבריונות. לעתים הוא נקרא "בריון", אבל מומחים למניעת בריונות ממליצים אף פעם לא לתייג אנשים כבריונים.

**הקורבן:** האדם שאליו מכוונת הבריונות או הפגיעה

**הצופה מהצד:** עד להטרדה או לבריונות שיודע על כך, ובוחר לא להתערב

**הצופה שמתערב:** עד להטרדה או לבריונות שתומך בקורבן בצורה חשאית או פומבית. לפעמים, הוא גם מנסה לעצור את האירוע ו/או לדווח על האירוע שראה

**להגביר:** להרחיב את מידת ההשתתפות או את מידת ההשפעה

**חרם:** סוג של הטרדה או בריונות באינטרנט ובמקומות אחרים. לרוב זה נקרא "חרם חברתי"

**לחסום:** שיטה להפסקת כל אינטראקציה עם אדם אחר באינטרנט, כדי שלא יוכל להיכנס לפרופיל שלכם, לשלוח לכם הודעות, לראות את הפוסטים שלכם וכו', בלי להודיע לו על כך (זו לא תמיד שיטה אידאלית במצבים של בריונות, כשהקורבן רוצה לדעת מה אומר הצד התוקף או מתי נפסקת ההתקפה)

**להשתיק:** זו שיטה פחות קיצונית מחסימה. אם התקשורת עם אדם אחר מפריעה לכם, באמצעות השתקה אפשר להפסיק לראות פוסטים, תגובות וכו' של האדם בפיד שלכם ברשת החברתית. האדם האחר לא מקבל הודעה על כך ואתם לא מושתקים בפיד שלו (לא מועיל במצבים של בריונות)

**אנונימי:** אדם שלא יודעים את שמו או שאינו מוכר. מישהו באינטרנט שלא יודעים את שמו ולא מכירים אותו

**הטרלה:** לפרסם תוכן או להגיב באינטרנט בצורה מרושעת, פוגענית או פרובוקטיבית, ובאופן מכוון

**דיווח על פגיעה:** שימוש במערכת או בכלים המקוונים של שירותי רשת חברתית כדי לדווח על הטרדה, בריונות, איומים או תוכן מזיק אחר שמפרים את התנאים וההגבלות או תקני הקהילה של השירות

# מגניב להיות אדיב: פעילות 1

## מהצופים מהצד לצופים שמתערבים

התלמידים מתרגלים זיהוי של ארבעת התפקידים במקרה של בריונות (הבריון, הקורבן, הצופה מהצד והצופה שמתערב) ומה לעשות אם הם צופים מהצד או קורבנות בעצמם.

### יעדים לתלמידים



- ✓ לזהות מצבים של הטרדה או בריונות ברשת.
- ✓ להעריך מה פירוש הדבר להיות צופה מהצד או צופה שמתערב באינטרנט.
- ✓ ללמוד דרכים ספציפיות שבהן אפשר להגיב לבריונות כשנתקלים בה.
- ✓ לדעת איך להתנהג כשמישהו מטריד אתכם.

### בואו נדבר



#### למה חשוב להיות אדיבים?

חשוב להזכיר לעצמנו שמאחורי כל שם משתמש ודמות יש אדם אמיתי עם רגשות אמיתיים, ועלינו להתייחס לאנשים כמו שהיינו רוצים שיתייחסו אלינו. במקרים של בריונות או התנהגות פוגענית אחרת מעורבים בדרך כלל אנשים מארבעה סוגים.

- התוקף, או האדם שמתנהג בבריונות
- האדם שאליו מכוונת הבריונות – הקורבן
- העדים למה שמתרחש, לרוב הם נקראים צופים מהצד
- עדים למה שמתרחש שמנסים להתערב בצורה חיובית, ונקראים צופים שמתערבים.

אם תהיו קורבנות של בריונות או התנהגות פוגענית אחרת באינטרנט, הנה כמה פעולות שתוכלו לבצע:

#### אם אתם הקורבנות, תוכלו...

- לא להגיב
- לחסום את האדם
- לדווח על התוקף – לספר להורה, למורה, לאח או אחות או למישהו אחר שסומכים עליו. כמו כן, כדאי להשתמש בכלי הדיווח שבאפליקציה או בשירות כדי לדווח על הפוסט, התגובה או התמונה הפוגעניים

אם אתם צופים מהצד כשמתרחשים מקרים של הטרדה או בריונות, אתם מסוגלים להתערב ולדווח על התנהגות מרושעת. לפעמים צופים מהצד לא מנסים להפסיק את הבריונות ולעזור לקורבן. כשהם כן מנסים – הם צופים שמתערבים. אפשר לבחור להיות צופים שמתערבים, אם מחליטים לא לתמוך בהתנהגות פוגענית ולקדם אדיבות וגישה חיובית. מעט גישה חיובית יכולה להשפיע בגדול באינטרנט. בעזרתה, אפשר לעצור הפצה של שליליות והתנהגות מרושעת ומזיקה.

#### כדי להפוך מצופים מהצד לצופים מתערבים, עלינו:

- למצוא דרך להיות אדיבים או לתמוך בקורבן
- להתריע על ההתנהגות הפוגענית באמצעות תגובה או תשובה (חשוב להתריע על ההתנהגות ולא על האדם), אם אתם מרגישים בנוח וחושבים שבטוח לעשות זאת
- להחליט שלא עוזרים לצד התוקף על ידי הפצת הבריונות או שיתוף הפוסט או התגובה הפוגעניים באינטרנט, כדי שהמצב לא יתדרדר
- לשכנע כמה חברים ליצור "ערימת אדיבות" – לפרסם הרבה תגובות טובות על הקורבן (ולא לפרסם משהו פוגעני על התוקף כי אתם רוצים לשמש דוגמה ולא לנקום בו)
- לדווח על ההטרדה. לספר למישהו שיכול לעזור, כמו הורה, מורה או יועץ/יועצת בבית הספר.

## פעילות



### החומרים הדרושים:

• דפי עבודה "מצופים מהצד לצופים שמתערבים"

תשובות לדף העבודה "מצופים מהצד לצופים שמתערבים"

תרחיש 1: צ, מ, צ (כי לא הוגשה עזרה), מ, מ

תרחיש 2: מ, צ, מ, מ

תרחיש 3: מ, מ, צ, צ, מ

תרחיש 4: התשובות שלכם!

### 1. קוראים תרחישים ומסווגים תגובות

לאחר דיון לגבי התפקידים, מחלקים את דפי העבודה ונותנים לתלמידים 15 דקות לקרוא את שלושת התרחישים ולסווג כל אחת מהתגובות. אם יהיה מספיק זמן, מבקשים מהם ליצור את התרחיש הרביעי ביחד בכיתה.

### 2. עורכים דיון על התשובות

לפני הדיון או בסופו, מבקשים מהם להסביר למה נחמד שיש צופים שמתערבים בבית הספר ובאינטרנט.

### 3. עורכים דיון על התגובות שהיה קשה לסווג

אם יש מספיק זמן, שואלים את התלמידים אם היה קשה לסווג תגובות מסוימות ומדוע. עורכים דיון בנושא.

## מה למדנו?

כשתרצו לעמוד לצד אחרים ולהגן עליהם, לדווח על התנהגות פוגענית או להתעלם ממה שהיה כדי שלא יתגבר, תוכלו לבחור מבין מגוון אסטרטגיות פעולה בהתאם למצב. בעזרת מעט אדיבות, כל אחד יכול להשפיע בגדול ולשנות מצבים שליליים לטובה.

# מעמדת הצופים מהצד לעמדת הצופים המתעריבים

עכשיו אתם יודעים שלצופים מהצד יש כוח להשפיע לטובה והם יכולים להיות צופים שמתעריבים, אם הם עוזרים לקורבן לבריונות. למטה מתוארים שלושה תרחישים כדוגמאות לבריונות או להטרדה באינטרנט. תוכלו גם ליצור תרחיש רביעי על סמך משהו שקרה לאנשים שאתם מכירים. חישבו על תגובות אפשריות לצופים שמתעריבים וגם לצופים מהצד. לכל אחד משלושת התרחישים הקיימים יש רשימת תגובות. עליכם לקרוא כל תגובה ולהחליט אם צופה מהצד היה מגיב כך, או צופה שמתערב. לאחר מכן, יש להזין "צ" עבור "צופה מהצד" או "מ" עבור "צופה שמתערב" בריבוע שלצד התגובה. אם יהיה זמן, תוכלו לערוך דיון בכיתה על התגובות שהיה קשה יותר להחליט לגביהן ועל הסיבות לכך.

## תרחיש 1

לחברה שלכם נפל הטלפון ליד הברזייה במגרש הכדורגל של בית הספר. מישהו מצא אותו ושלח הודעה פוגעת מאוד על תלמיד אחר לאנשים בקבוצת הכדורגל שלה. אחר כך, הוא החזיר את הטלפון למקום שבו נפל. הקורבן אמר לחברה שהיא ממש מגעילה בעקבות ההודעה ששלחה, למרות שלא היא שלחה אותה. אף אחד לא יודע מי שלח את ההודעה הפוגעת. אתם...

- ☐ עצובים בגלל המצב אבל לא עושים כלום, כי אף אחד לא יודע מי פגע בה.
- ☐ מחפשים את הקורבן ושואלים אותו איך הוא מרגיש ואם אתם יכולים לעזור.
- ☐ מפיצים את הדרמה על ידי שיתוף ההודעה הפוגעת עם חברים אחרים.
- ☐ והחברה משכנעים את כל חברי קבוצת הכדורגל לפרסם מחמאות על הקורבן.
- ☐ והחברה מדווחים על האירוע באופן אנונימי למנהל בית הספר, ומבקשים שכולם ידברו על אבטחת הטלפונים ונעילתם.

## תרחיש 2

המורה יצרה בלוג כיתתי למקצוע השפה כדי שתלמידי הכיתה יוכלו לכתוב, לערוך ולפרסם תגובות. למחרת, המורה חולה והמורה המחליף לא שם לב שיש בעיה בבלוג – מישהו מפרסם תגובות פוגעניות ביותר על אחד התלמידים בכיתה. אתם...

- ☐ מגיבים לתגובות כך "זה ממש לא מגניב" ו"אנחנו חברים של \_\_\_\_\_, וזה לא נכון".
- ☐ מתעלמים מהתגובות עד שהמורה חוזרת.
- ☐ משכנעים תלמידים אחרים לפרסם תגובות חיוביות ומחמאות על התלמיד הקורבן.
- ☐ מדווחים למורה המחליף על ההתנהגות הפוגעת בבלוג הכיתתי, ושהוא יכול לדווח על כך למורה.

### תרחיש 3

יש משחק באינטרנט שהחברים שלכם משחקים בו הרבה. בדרך כלל, בצ'אט של המשחק מדברים על מה שקורה במשחק. לפעמים ההערות קצת קשות, אבל הן קשורות לתחרות בין החברים ולא לתוכן פוגעני. אבל הפעם, אחד השחקנים מתחיל לכתוב תוכן פוגע מאוד על אחד החברים שלכם שגם משחק, והוא לא מפסיק עם זה. הוא אפילו ממשיך גם למחרת. אתם...

- ☐ מתקשרים לחבר ואומרים שאתם לא מרוצים מזה, ושואלים מה לדעתו אתם צריכים לעשות.
- ☐ מתקשרים לכל מי שאתם מכירים מהמשחק (ומוודאים שהחבר יודע שאתם עושים זאת), כדי לשכנע אותם שהגיע הזמן להעיר על ההתנהגות הפוגענית.
- ☐ מחליטים לחכות ולראות אם התלמיד יפסיק, ואולי לעשות משהו לאחר מכן.
- ☐ יוצאים מהמשחק לזמן-מה.
- ☐ מחפשים את כללי הקהילה של המשחק, ואם בריונות אסורה, מדווחים על ההתנהגות המרושעת באמצעות מערכת הדיווח של המשחק.

### תרחיש 4

יוצרים תרחיש אמיתי ביחד בכיתה, על סמך מצב שאחד מכם שמע עליו. לאחר מכן, חושבים על תגובות של צופים מהצד וצופים שמתערבים כדי להראות שהפנמתם את מה שדיברנו עליו כאן!

## מגניב להיות אדיב: פעילות 2

# אפשרויות לצופים שמתערבים

לרוב, תלמידים רוצים לעזור לקורבן לבריונות אבל לא יודעים מה לעשות. בעזרת הפעילות הזו, הם רואים שיש אפשרויות, קוראים דוגמאות ומקבלים הזדמנות ליצור תגובות חיוביות משלהם.

### יעדים לתלמידים



- ✓ להבין שאפשר לבחור להיות צופים שמתערבים
- ✓ ללמוד שיש דרכים שונות להתערב במצב מסוים
- ✓ לבחור איך להגיב מתוך מספר אפשרויות שמתאימות לכם ושאתם מרגישים איתן בנוח
- ✓ ליצור תגובה משלכם למצב.

### בואו נדבר



כשאתם עדים להתנהגות פוגענית של מישהו כלפי אדם אחר באינטרנט – כשהוא גורם לו להרגיש נבוך או לא שייך, צוחק עליו, מזלזל בו, פוגע בו וכו', תמיד יש לכם אפשרויות פעולה. תחילה, אתם יכולים לעזור לקורבן וכך להיות צופים שמתערבים במקום צופים מהצד. שנית, אם תבחרו להיות צופים שמתערבים, יש כמה סוגי פעולות שתוכלו לבצע.

הדבר הכי חשוב לדעת הוא שאפשר להקשיב לקורבן וכך לעזור לו אם הוא עצוב, כי הוא יודע שלמישהו איכפת ממנו.

- לא כולם מרגישים בנוח לתמוך באנשים **פומבי**, בין אם זה באינטרנט או בקפוטריה של בית הספר. אם אתם מרגישים בנוח, לכו על זה! אפשר...
- להעיר על ההתנהגות הפוגענית (ולא על האדם שפוגע) ולומר שזה לא מגניב
- לכתוב משהו חיובי על הקורבן בפוסט או בתגובה
- לשכנע חברים לכתוב מחמאות לקורבן באינטרנט
- אפשר להזמין את האדם לשחק איתכם בגן המשחקים או לשבת איתכם בארוחת הצהריים.

אם אתם לא מרגישים בנוח לעזור באופן פומבי, זה בסדר. תוכלו לתמוך בקורבן גם בצורה **פרטית**. אפשר...

- לשאול איך הוא מרגיש בהודעת טקסט או בהודעה ישירה
- לכתוב הערה חיובית או מחמאה בפוסט, בתגובה או בהודעה באופן אנונימי (אם אתם משתמשים במדיה שמאפשרת להיות אנונימי)
- לומר לו שאתם נמצאים כאן אם הוא רוצה לדבר אחרי שעות בית הספר
- בשיחה רגועה פנים-אל-פנים או בטלפון, אומרים לו שלדעתכם ההתנהגות הפוגעת לא הולמת ושואלים אם הוא רוצה לדבר על מה שקרה.

בכל דרך שבה תבחרו להיות צופים שמתערבים, יש אפשרויות **דיווח** באופן ציבורי ופרטי. פירוש הדבר שניתן לדווח על בריונות דרך אתר או ממשק אפליקציה, או לדווח למבוגר שאתם סומכים עליו.

## פעילות



### החומרים הדרושים:

- לוח עם משטח לבן גדול שעליו יכולים תלמידים להדביק פתקיות דביקות
- דפי עבודה "אפשרויות לצופים שמתערבים"
- פתקיות דביקות לכל קבוצת תלמידים

בפעילות זו ננסה לראות איך זה להיות צופים שמתערבים. בואו נניח שכל הכיתה החליטה לעזור לקורבן.

**1. מתחלקים לקבוצות עם חמישה תלמידים בכל קבוצה**  
כל קבוצה צריכה לבחור קורא וכותב.

**2. חברי הקבוצה קוראים את תיאור המצבים הפוגעניים ועורכים עליהם דיון משותף**  
שלושת המצבים מתוארים בדף העבודה שבעמוד הבא.

בזמן הדיונים הקבוצתיים, המורה מחלקת את הלוח לשני חלקים גדולים עם הכותרות "תמיכה פומבית" ו"תמיכה פרטית".

**3. הקבוצות בוחרות את שני סוגי התגובות לכל מצב**  
התלמידים יכולים להשתמש בתגובות לדוגמה שבקטע "בואו נדבר", או ליצור תגובות משלהם.

**4. התלמידים כותבים על הלוח את התגובות שבחרו ומקריאים בקול לכל הכיתה**  
המורה יכולה לנהל דיון כיתתי על סמך הבחירות של התלמידים.

## מה למדנו?

פעמים רבות, כשאתם רואים שפוגעים במישהו או מטרידים אותו, אתם רוצים לעזור אבל לא יודעים מה לעשות. בשלב זה, אתם כבר מכירים דרכים רבות לעזור לקורבן ויודעים שאפשר לתמוך בו בדרך שאתם מרגישים בנוח איתה. אתם מסוגלים לעזור לאנשים בדרך שמתאימה לכם!



## דף עבודה: פעילות 2

# אפשרויות לצופים שמתערבים

עכשיו אתם עובדים בקבוצות, וכל קבוצה מחליטה איך חבריה רוצים להיות צופים שמתערבים. מבקשים מתנדב אחד בקבוצה שיכתוב (על הפתקיות הדביקות) ומתנדב אחד שיקרא. הקורא מקריא את המצב הראשון. לקבוצות יש חמש דקות כדי לדון בכל מצב ולהחליט איך יתמכו בקורבן בפומבי ואיך יתמכו בו באופן פרטי. הכותב כותב את ההחלטות על שתי פתקיות דביקות ומדביק אחת מהן בעמודה "פומבי" ואת השנייה בעמודה "פרטי" על הלוח. כדי להגיע להחלטה, אפשר להשתמש ברעיונות שנדונו עכשיו בכיתה או להעלות רעיונות משלכם לעזרה לקורבן. חוזרים על התהליך גם למצב 2 ומצב 3.

הערה: יש יותר מדרך אחת נכונה לתמוך בקורבן, כי כל אדם (הקורבן וגם הצופה מהצד) הוא שונה וכל מצב הוא שונה. אנחנו פשוט מנסים אפשרויות שונות לצופים שמתערבים.

### מצב 1

תלמיד מפרסם סרטון שבו הוא שר קאבר לשיר מפורסם של זמר פופ. תלמידים אחרים מתחילים לפרסם תגובות פוגעניות מתחת לסרטון. איך אתם יכולים לתמוך בתלמיד שפרסם את הסרטון? היעזרו בחלק מהרעיונות שדנו בהם או החליטו על התגובה של הקבוצה.

### מצב 2

תלמידה שולחת לתלמידה אחרת צילום מסך של תגובה שפרסם חבר שלכם וכותבת בדיחה פוגענית לגביה. צילום המסך מתפרסם מחדש והופך לפוסט ויראלי בבית הספר. איך תתמכו בתלמיד שצילום המסך של תגובתו שותף? אפשר לבחור אחד מהרעיונות שערכנו עליהם עכשיו בדיון בכיתה, או להחליט על תגובה משלכם.

### מצב 3

גיליתם שתלמיד בבית הספר שלכם יצר חשבון מזויף ברשת החברתית, עם שם של תלמיד אחר. הוא פרסם תמונות וממים שכוללים הערות פוגעניות על תלמידים, על מורים ועל בית הספר. מה תחליטו לעשות כדי לתמוך בתלמיד שאליו מתחזים בצורה זו? אפשר לשקול חלק מהרעיונות שכבר דנו בהם או להחליט על תגובה משלכם.

# מגניב להיות אדיב: פעילות 3

## ...אבל תגידו את זה בצורה יפה!

בפעילות הזו, התלמידים עובדים יחד ומנסחים מחדש הערות שליליות, כדי ללמוד איך להפוך אינטראקציות שליליות לחיוביות.

### יעדים לתלמידים



- ✓ לבטא רגשות ודעות בדרכים חיוביות ויעילות
- ✓ להגיב לשליליות בצורה מנומסת ובונה.

### בואו נדבר



#### איך הופכים את השלילי לחיובי

- ילדים בגילכם חשופים למגוון רחב של תכנים באינטרנט. חלק מהתכנים האלה עלולים לכלול מסרים שליליים שמעודדים התנהגות פוגענית.
- האם אתם (או מישהו שאתם מכירים) נתקלתם במישהו שהתנהג בצורה שלילית באינטרנט? איך הרגשתם בנוגע לכך?
  - האם חוויתם התנהגות אדיבה באינטרנט, או שמישהו שאתם מכירים חווה זאת? איך הרגשתם בנוגע לכך?
  - אילו פעולות פשוטות אנחנו יכולים לבצע כדי להפוך אינטראקציות שליליות לחיוביות?
- אנחנו יכולים להגיב לרגשות שליליים בדרכים בונות, על ידי ניסוח מחדש של הערות פוגעניות, ובכך שנהיה מודעים יותר לטון המשתמע בתקשורת שלנו באינטרנט.

### פעילות



#### 1. קוראים את התגובות

בוחנים את התגובות השליליות.

#### 2. כותבים תיקונים

- נתפצל עכשיו לצוותים של שלושה אנשים ונעבוד על שני סוגים של תגובות להערות האלה:
- איך הייתם יכולים להעביר את אותם המסרים, או מסרים דומים, בדרכים חיוביות ובונות יותר?
  - אם אחד מחבריכם לכיתה מעיר הערות כאלה, איך תוכלו להשיב לו כך שהשיחה תהיה חיובית יותר?

#### הערה למורה

ייתכן שתלמידים צעירים יצטרכו דוגמאות כדי לראות איך לשנות תגובות. אחת הדרכים היא להשלים דוגמה אחת ביחד עם הכיתה, כך שהתלמידים יוכלו להצליח במשימה גם כשיעבדו באופן עצמאי.

#### 3. מציגים את התגובות

כל קבוצה מציגה את התגובות שלה לשני המצבים.

#### החומרים הדרושים:

- לוח או מסך הקרנה
- דפי עבודה "אבל תגידו את זה בצורה יפה!" גיליון עבודה
- פתקיות דביקות או מכשירים לתלמידים

### מה למדנו?

תגובה חיובית למשהו שלילי יכולה להוביל לשיחה מעניינת ומהנה יותר, וזה הרבה יותר טוב ממצב שנוצר בעקבות הערה לא נעימה.

# ... אבל תגידו את זה בצורה יפה!

קיראו את התגובות שבהמשך. לאחר כל תגובה, דונו בשאלות האלה:

1. איך הייתם יכולים להעביר את אותם המסרים, או מסרים דומים, בדרכים חיוביות ובונות יותר?
2. אם אחד מחבריכם לכיתה מעיר הערות כמו אלה, איך תוכלו להשיב לו כך שהשיחה תהיה חיובית יותר?

השתמשו בשורות שמתחת לכל תגובה כדי לכתוב רעיונות.

חחח דניאל הוא היחיד בכיתה שלא ישתתף  
בטיול השנתי.

כולם לובשים סגול מחר, אבל אל תספרו  
ליעל.

מצטערת, אני לא חושבת שאת יכולה לבוא למסיבה  
שלי. זה יעלה יותר מדי כסף.

אל תיעלב, אבל כתב היד שלך מביך. עדיף שתצטרף לקבוצה  
אחרת לעבודה על הפרויקט הזה.

איזו זוועה – מי אמר לה שהיא שרה  
יפה??

תוכל להצטרף לקבוצה שלנו רק אם  
תיתן לי את פרטי הכניסה לחשבון שלך.

אני היחידה שחושבת שמורן נראית קצת  
כמו דרדסית?



## מגניב להיות אדיב: פעילות 4

# שימו לב לטון שלכם

התלמידים מפרשים את הרגשות שמאחורי הודעות טקסט, כדי לתרגל חשיבה ביקורתית והימנעות מפרשנות שגויה וקונפליקטים בחילופי דברים באינטרנט.

### יעדים לתלמידים



- ✓ **לקבל החלטות נכונות** כשבחרים איך לתקשר ואיזה מסר רוצים להעביר, ומתי לא כדאי להעביר מסר כלשהו.
- ✓ **לזהות מצבים** שבהם עדיף לחכות עד שתוכלו לדבר עם החבר פנים אל פנים, במקום לשלוח הודעות מייד

### בואו נדבר



**קל לפרש משהו בצורה שגויה**  
צעירים משתמשים בסוגים שונים של תקשורת לסוגי אינטראקציות שונים, אבל הודעות צ'אט או טקסט עשויות להתפרש באופן שונה מאשר אילו הדברים היו נאמרים פנים אל פנים או בטלפון.  
האם קרה לכם שלא הבינו אתכם נכון בהודעת טקסט? לדוגמה, האם שלחתם פעם הודעה עם בדיחה, והחבר שלכם חשב שהתכוונתם ברצינות או שזה היה פוגעני?  
האם קרה לכם שלא הבנתם נכון מישהו אחר בהודעת טקסט או בצ'אט? מה עשיתם כדי להבהיר את המסר? מה הייתם יכולים לעשות אחרת?

### פעילות



#### החומרים הדרושים:

- הודעות טקסט לדוגמה, כתובות על הלוח או מוקרנות

#### 1. סוקרים את ההודעות

- בואו נבחן את הודעות הטקסט לדוגמה שכתובות על הלוח. לתלמידים בכיתה בטח יש עוד דוגמאות טובות. בואו נכתוב אותן על הלוח ונערוך דיון.
- "זה ממש מגניב"
  - "ווטאבר"
  - "אני ממש כועס עליך"
  - "תתקשרי אליי עכשיו"
  - "בסדר"

#### 2. קוראים את ההודעות בקול

עכשיו אני אבקש כל פעם ממישהו אחר להקריא בקול הודעה בטון ספציפי (למשל, 😊 😐 😞).

במה הבחנתם? איך אנשים אחרים יכולים לפרש את ההודעות האלה? איך השולח של כל אחת מההודעות יכול להעביר טוב יותר את הכוונה האמיתית שלו?

### מה למדנו?

קשה להבין איך מישהו מרגיש באמת כשקוראים את מה שהוא כתב בהודעה. הקפידו לבחור את אמצעי התקשורת הנכון להעברת המסר שלכם – ולא לקפוץ למסקנות מדברים שאנשים כותבים לכם באינטרנט. אם אתם לא בטוחים למה התכוון כותב ההודעה, תוכלו לדבר איתו פנים אל פנים או בטלפון כדי לברר.

## מגניב להיות אדיב: פעילות 5

# להתנהג בהתאם

התלמידים מדברים על כך שילדים יכולים לשמש מודל לחיקוי גם למבוגרים.

### יעדים לתלמידים



- ✓ לדון בהתנהגות של מבוגרים באינטרנט
- ✓ לבחון כיצד ההתנהלות של המבוגרים יכולה לעצב את ההתנהגות של הדור הצעיר.

### בואו נדבר



#### מה מבוגרים יכולים ללמד ילדים – ומה ילדים יכולים ללמד מבוגרים!

חשוב לחנך לאדיבות. עם זאת, לא פחות חשוב לשמש דוגמה להתנהגות אדיבה שעליה אנחנו מלמדים. יש דוגמאות רבות שממחישות שבריונות והטרדה הן לא בעיות של ילדים בלבד. תראו למשל איך מבוגרים מתייחסים זה לזה באינטרנט, בשידורי חדשות או בפקקי תנועה.

דיברנו על החשיבות של הפגנת אדיבות כלפי חברים לכיתה וחברים באינטרנט ובחיים האמיתיים. האם ראיתם פעם מבוגרים שמתנהגים בצורה שלילית זה לזה? האם ראיתם מבוגרים שמתנהגים בבריונות זה כלפי זה? (זכרו, אין צורך לנקוב בשמות – אנחנו רוצים לדבר רק על ההתנהגות)

האם לדעתכם הדור שלכם יכול לבנות סביבת אינטרנט נעימה וחיונית יותר מאשר הסביבות שמבוגרים מסוימים יצרו עבור עצמם? (מבוגרים רבים חושבים שבטח גם בזה תהיו טובים יותר.) מה אפשר לעשות כדי ליצור אווירה חיובית ונעימה יותר באינטרנט? למשל: לתת לייקים או תגובות חיוביות לאנשים שתורמים תוכן יצירתי ורעיונות ברשת, לתרום מהידע שלנו לאחרים, כשנותנים ביקורת – לכתוב ביקורת עניינית ומנומסת (לא לקלל ולא לרדת לפסים אישיים).

האם אתם חושבים שיש ילדים שמתנהגים בבריונות או מעירים הערות פוגעניות בגלל שהם רואים מבוגרים בסביבתם, או בשידורי חדשות, שמתנהגים בצורה כזו? עניתם "כן" לכל השאלות האלה? כדאי לתת דוגמאות. מה אתם הייתם עושים אחרת – איך תוכלו לשמש מודל טוב יותר למבוגרים?

#### הערה למורה

אפשר ליצור "קמפיין אדיבות" בבית הספר כדי לקדם את הדיון הזה! בתחילת שיעור כלשהו, כל תלמיד כותב פתק עם הודעה חיובית ומעביר אותו לתלמיד אחר. מטרת הפעולה היא להכתיב טון חיובי לשיעור בכיתה וגם לשמש תזכורת לכך שאנחנו יכולים להקרין גישה חיובית באינטרנט ובחיים. אפשר אפילו להתחיל שיעור ככה בכל שבוע!

### מה למדנו?

לאופן שבו אתם והחברים שלכם מתייחסים זה לזה באינטרנט תהיה השפעה רבה על העולם הדיגיטלי שהדור שלכם בונה – וכמובן על העולם האמיתי שאינו מקוון.

## ממלכת האינטרנט: ממלכת האדיבות

קל להפיץ רגשות מכל הסוגים, לטוב ולרע. בפינה שטופת השמש של העיירה, תוקפים מתרועעים בטירוף ומפיצים שליליות לכל עבר. עליכם לחסום את התוקפים ולדווח עליהם כדי לעצור את ההשתלטות העוינת. כדאי להיות אדיבים כלפי רשתונים אחרים כדי לחזור לאופי הרגוע של הממלכה.

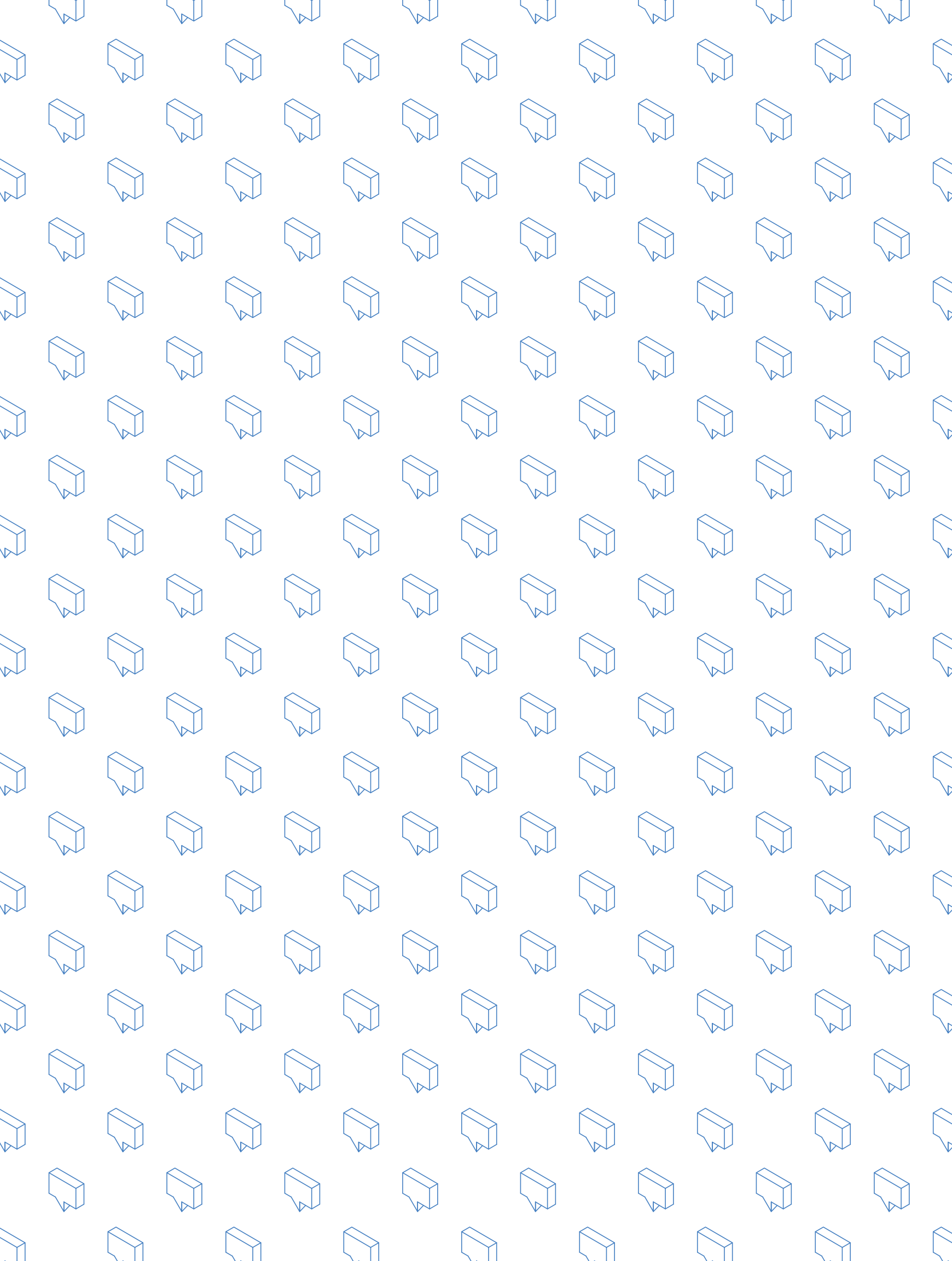
יש לפתוח דפדפן אינטרנט במחשב או בנייד שלכם (לדוגמה, בטאבלט) ולהיכנס אל [g.co/KindKingdom](http://g.co/KindKingdom).

### נושאים לדיון



- התלמידים ישחקו ב"ממלכת האדיבות" ובעזרת השאלות הבאות, ידונו במה שהם למדו מהמשחק. רוב התלמידים מפקים את מירב התועלת ממשחק עצמאי, אבל התלמידים יכולים גם לשחק בזוגות. זה יכול לעזור במיוחד לתלמידים צעירים.
- עם איזה תרחיש בממלכת האדיבות אתם מזדהים במידה הרבה ביותר, ומדוע?
  - תארו מצב שבו הפצתם אדיבות כלפי אחרים באינטרנט
  - באיזה מצב מתאים לחסום מישהו באינטרנט?
  - באיזה מצב מתאים לדווח על התנהגות של אדם כלשהו?
  - למה לדעתכם הדמות בממלכת האדיבות נקראת "תוקפת"? תארו את תכונות הדמות ואיך הפעולות שלה משפיעות על המשחק.
  - בעקבות המשחק ב"ממלכת האדיבות", האם השתנה האופן שבו תתנהגו לאחרים? אם כן, כיצד?

## הערות





# אם לא בטוחים, מדווחים

## הגדרה ועידוד של התנהגות אמיצה באינטרנט

### סקירה כללית של השיעור

פעילות 1: מתי כדאי לבקש עזרה  
פעילות 2: מדווחים על זה גם באינטרנט

### הרעיונות העיקריים

חשוב שילדים יבינו שהם לא לבד כשהם רואים באינטרנט תוכן שהם לא מרגישים בנוח איתו – במיוחד אם נראה שהם עלולים להיפגע, או שמשהו אחר עלול להיפגע. הם צריכים לבקש עזרה ממישהו שהם סומכים עליו, בלי להסס. כמו כן, כדאי שהם ידעו שיש דרכים שונות להפגין אומץ ולנקוט פעולה, משיחה לא מקוונת ועד שימוש בכלי דיווח מקוונים.

### יעדים לתלמידים

- ✓ להבין באילו סוגי מצבים צריך לבקש עזרה או לדבר עם מבוגר שסומכים עליו.
- ✓ לבחון אילו אפשרויות קיימות להתנהגות אמיצה, ולמה חשוב לשתף מבוגרים.

### תקנים רלוונטיים

תקני ISTE לנשות חינוך ולאנשי חינוך: 1c, 2c, c3, a3, b3, b4, a5, 5b, 6a, b6 6d, a7  
תקני ISTE לתלמידים 2016: 1c, 2b, 3d, 4d, 6a, 7a, 7b, 7c  
תקני למידה של AASL: I.a.1, I.b.1, I.b.2, 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.d.1, II.d.2, II.d.3, 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.2, IV.b.3, 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.a.3, VI.d.1, VI.d.3

# אם לא בטוחים, מדווחים

## אוצר מילים



**אמיצים:** ולא בהכרח חסרי מורא, כי אנשים מתנהגים באומץ במיוחד כשהם מפחדים או חוששים, ונוקטים פעולה חיובית למרות זאת

**חשבון פרוץ:** חשבון מקוון שמישהו אחר השתלט עליו, כך שאין לכם יותר שליטה מלאה עליו

**יכולת פעולה עצמאית של התלמיד:** מעבר ליכולת רק לדבר. היכולת לפעול או לבצע שינוי, כולל להגן על עצמכם או על אחרים. בדרך כלל, יכולת זו היא חלק חשוב מהאזרחות

**אמון:** אמונה חזקה שמישהו או מישהו הם אמיתיים, נכונים ואפשר לסמוך עליהם

## אם לא בטוחים, מדווחים: פעילות 1

# מתי כדאי לבקש עזרה

אחת העצות שמופיעה בעקביות בשיעורים האלה היא זו: אם תלמידים נתקלים במשהו שהם לא מרגישים איתו בנוח או שהם מרגישים תחושות קשות יותר, יש לעודד אותם לדווח על כך. הם צריכים להיות אמיצים ולדבר עם מישהו שסומכים עליו ויכול לעזור – כולל אתם המורים, המנהל או הורה. התלמידים אמורים להבין את הנקודה הזאת מכל אחד מהשיעורים. ליתר ביטחון, יש כאן דיון כיתתי שממוקד בעיקרון "אם לא בטוחים, מדווחים". למטה תמצאו רשימת מצבים שבהם שיחה עם מישהו יכולה לעזור מאוד.

### הערות חשובות לנשות חינוך ולאנשי חינוך

1. דורות רבים של ילדים חונכו לא "להלשין" על אחרים, וכיום זו הנורמה החברתית. מומחים למניעת בריונות משקיעים מאמצים רבים כדי לעזור לילדים להבין את ההבדל בין "הלשנה" לבקשת עזרה. עיזרו לתלמידים שלכם להבין שכשמתרחשת פגיעה באינטרנט ומישהו צריך תמיכה, זה לא קשור להלשנה, אלא לקבלת עזרה עבורם או עבור חברים שלהם שנפגעו.

2. אם תעודדו תקשורת פתוחה בכיתה ותזכירו לתלמידים שאתם שם בשביל לתמוך בהם, אתם תתרמו ליכולת של התלמידים לפעול בצורה עצמאית ולדווח בהתאם.

3. בדיון שמתואר למטה, בכל פעם שתלמידים משתפים מצבים שבהם ביקשו עזרה ממבוגר, חשוב שטון השיחה יגרום להם להרגיש גאים ואמיצים בעקבות הפעולה שנקטו. הדבר חשוב במיוחד כי הם מדברים בפני חברים לכיתה.

### יעדים לתלמידים



- ✓ להבין שבקשת עזרה לעצמכם או לאחרים היא סימן לכוח.
- ✓ לדון יחד במצבים שבהם שיחה יכולה לעזור לכם מאוד.

### בואו נדבר



הנה רשימת מצבים שאתם עשויים להיתקל בהם באינטרנט. אולי לא נעבור על כולם. אני מקווה שתרימו את היד כשמישהו ברשימה יזכיר לכם מצב שחוויתם ואיך הגבתם. כך נוכל לדבר על המצבים האלה.

## מה למדנו?

אולי זה לא נראה כך, אבל נדרש אומץ כדי לבקש עזרה כשלא יודעים מה לעשות. אולי אתם רוצים להתגבר על משהו שפגע בכם, לעזור למישהו אחר שנפגע או למנוע פגיעה – זו התנהגות חכמה ואמיצה.

## נושאים לדיון



### 1. כל אחד קורא בשקט את הרשימה לעצמו. בזמן שקוראים, חושבים אם המצבים האלה קרו לכם,

- אם רציתם לבקש עזרה ממבוגר ואם ביקשתם עזרה בסופו של דבר או לא.
- חשדתם שהחשבון שלכם נפרץ (הזדמנות לדיון: מה ניתן לעשות כדי לשפר את אבטחת החשבון?)
- הייתם צריכים עזרה כדי להיזכר בסיסמה
- לא הייתם בטוחים אם נתקלתם בתרמית או שחשבתם שנפלתם קורבן לתרמית (הזדמנות לדיון: מהם סימני האזהרה?)
- מישהו ניסה לדבר איתכם באינטרנט על משהו שלא הרגשתם איתו בנוח
- קיבלתם הודעה או תגובה מפחידה מאדם זר (הזדמנות לדיון: למה תוכן יכול להיראות מפחיד?)
- רציתם לדבר על משהו ממש נעים או ממש פוגע, שמישהו אמר באינטרנט
- דאגתם ששיתפתם תוכן באינטרנט שלא הייתם אמורים לשתף. ספרו לנו מה זה היה רק אם אתם מרגישים בנוח לגבי שיתוף התוכן עם הכיתה. גם אם לא תשתפו איתנו, ספרו לנו מה עשיתם לאחר מכן.
- ראיתם מישהו שאתם מכירים פוגע בתלמיד אחר באינטרנט
- ראיתם מישהו מאיים להכות מישהו אחר או לפגוע בו
- מישהו פרסם פרופיל מזויף על תלמיד אחר
- דאגתם לשלומם של תלמיד אחר בגלל תוכן שהוא פרסם או שלח בהודעת טקסט (הזדמנות לדיון: לפעמים לא רוצים להסתכן בכך שהחבר יתעצבן, אבל האם הרווחה והבטיחות שלו אינם אמורים להיות חשובים יותר?).

### 2. מרימים את היד אם רוצים לספר לנו מה עשיתם (או לא עשיתם) ומדוע. אם מישהו כבר בחר באפשרות מסוימת, בידקו אם יש אפשרות אחרת שנוכל לדבר עליה.

### 3. בואו נערוך דיון על המצבים האלה.

## הערה למנהלי התוכנית

אחת הדרכים היעילות לפתח את היכולת של התלמידים לפעול בצורה עצמאית היא להקים פאנל או קבוצת עבודה של תלמידים בבית הספר (או בחטיבה/בתיכון). אם כבר קיימים פאנל או קבוצת עבודה בבית הספר, המנטורים יכולים לעבור על התרחישים שלמעלה עם תלמידים צעירים יותר ולשתף אותם בחוויות האישיות שלהם בנוגע לתרחישים.

## אם לא בטוחים, מדווחים: פעילות 2

# מדווחים על זה גם באינטרנט

באמצעות מכשיר של בית הספר שנועד להדגים לאן להיכנס כדי לדווח על התנהגות ותוכן בלתי הולמים באפליקציות, תלמידי הכיתה בוחנים סוגי תוכן שונים. הם מחליטים אם צריך לדווח על התוכן ומדברים על הסיבות לדיווח או אי-דיווח.

### יעדים לתלמידים



- ✓ להיות מודעים לכלים מקוונים לדיווח על פגיעה
- ✓ לשקול מתי להשתמש בהם
- ✓ לדבר על הסיבות לדיווח על פגיעה ועל המצבים שבהם כדאי לדווח על כך.

### בואו נדבר



כשתוכן פוגעני ותוכן אחר שאינו הולם מופיע באינטרנט, אפשר לנקוט פעולה במספר דרכים. בפעילות האחרונה דיברנו על האפשרות החשובה ביותר: לדבר על זה עם מישהו שאתם סומכים עליו. אפשרות נוספת היא לדווח על כך באפליקציה או בשירות שבה הופיע התוכן, וכך לגרום למחיקת התוכן. חשוב להתרגל לשימוש בכלי דיווח באינטרנט.

תלמידים צריכים להתרגל לצלם צילום מסך של פעילות או שיחות פוגעניות או חשודות, לפני השימוש בכלים לחסימה ולדיווח (כי בעקבות השימוש בכלים אלה, ייתכן שתיעוד הפעילות לא יהיה נגיש). כך ניתן להבטיח שמבוגרים אמינים יראו מה קרה ויעזרו לפתור את העניין.

### פעילות



#### החומרים הדרושים:

ידפי עבודה "מדווחים על זה גם באינטרנט"

#### 1. מגלים איך לדווח על בעיה

מוצאים את כל המכשירים שלכיתה יש גישה אליהם. אם יש מספר מכשירים, מחלקים את הכיתה לקבוצות. ביחד, מוצאים את הכלים בשלושה חשבונות לפחות שקשורים לבית הספר, כדי לדווח על תוכן או התנהגות בלתי הולמים (אם יש רק מכשיר או מחשב אחד בחדר, כל קבוצת תלמידים תעבוד בתורה על המסך הקיים).

#### 2. עוברים על התרחישים

כל התלמידים עוברים ביחד על שבעת המצבים שבדף העבודה.

#### 3. הייתם מדווחים על כך?

מבקשים מהתלמידים שהיו מדווחים על התוכן להרים ידיים. לאחר מכן, מבקשים מהתלמידים שלא היו מדווחים – להרים ידיים.

#### 4. אם כן, למה?

מבקשים ממישהו שהיה מדווח, לספר לכיתה את הסיבה לכך. מבקשים גם ממישהו שלא היה מדווח, לספר לכיתה את הסיבה לכך.

הערה: לעתים רחוקות יש רק תשובה אחת נכונה, או רק גישה אחת נכונה. חשוב לוודא שתלמידי הכיתה מודעים לזה לפני שמתחילים את הדיון.

## מה למדנו?

רוב האפליקציות והשירותים כוללים כלים לדיווח על תוכן בלתי הולם ו/או חסימה שלו. אם נשתמש בכלים האלה, נוכל לעזור לאנשים המעורבים, לקהילה שלהם ולפלטפורמות. לפני שחוסמים תוכן בלתי הולם או מדווחים עליו, כדאי לצלם צילום מסך כדי שיהיה תיעוד של המצב.

## דף עבודה: פעילות 2

# מדווחים על זה גם באינטרנט

קיראו כל אחד מהתרחישים שלמטה והרימו את היד אם הייתם מדווחים עליו באפליקציה או בשירות שבהם נתקלתם בו. יהיה עליכם להסביר למה הייתם מדווחים או לא הייתם מדווחים על כך, ולאחר מכן נדון בבחירות שלכם בכיתה.

הערה: כולם צריכים לדעת שרק לעתים רחוקות יש בחירה אחת נכונה, ולכן חשוב לערוך דיון בכיתה. אף אחד לא צריך להרגיש שהבחירה שלו לא טובה. אפילו מבוגרים לא תמיד יודעים מתי כדאי לדווח, או איך לדווח.

### מצב 1

תלמיד מפרסם תמונה קבוצתית בחשבון ציבורי, ואתם לא מרוצים מהמראה שלכם בתמונה. הייתם מדווחים על התמונה או לא? איך אפשר להגיב?

### מצב 2

מישהו יוצר חשבון של תלמיד שאתם מכירים עם השם והתמונה שלו. הוא יוצר מם מהתמונה ומצייר שפם ועוד מאפיינים מוזרים על הפנים, כך שהתמונה הופכת לבדיחה. הייתם מדווחים על החשבון או לא?

### מצב 3

מישהו מפרסם באופן אנונימי הרבה תגובות פוגעניות על תלמיד בבית הספר שלכם, ויש לכם הרגשה שאתם יודעים מי זה. הייתם מדווחים על התגובות או לא?

### מצב 4

תלמיד יוצר חשבון עם שם בית הספר כשם התצוגה ומפרסם תמונות של תלמידים עם תגובות שכולם שומעים עליהן. חלק מהתגובות פוגעניות כלפי תלמידים וחלק מהן – מחמאות. האם אתם מדווחים על התגובות הפוגעניות, על כל החשבון או על שניהם?

### מצב 5

ערב אחד, אתם רואים תגובה של תלמיד באינטרנט שאומר שהוא ילך מכות עם תלמיד אחר בקפיטריה ביום שלמחרת. האם תדווחו על התגובה הזו באינטרנט או לא? האם תדווחו על כך למורה או למנהל/ת בבוקר שלמחרת או לא? האם תדווחו בשני הערוצים?

### מצב 6

אתם צופים בסרט מצויר. פתאום רואים שם תוכן מוזר שלא מתאים לילדים ואתם מרגישים לא נוח. האם תדווחו על כך?

### מצב 7

אתם משחקים עם חברים במשחק באינטרנט, ומישהו שאף אחד לא מכיר מתחיל לדבר איתכם בצ'אט. הדברים שהאדם אומר לא מעליבים, אבל אתם לא מכירים אותו. האם תתעלמו ממנו או תדווחו עליו?

## הערות





