משרד החינוך
מנהל תקשוב, טכנולוגיה ומערכות מידע
אגף טכנולוגיות מידע

Login מפתח האבטחה שלי ״ סי@מה מושלמת״

Password **********

☐ Save login and password

Apply

המפתח להגנה על ילדים באינטרנט הוא לחנך אותם על הסכנות שהם עלולים לחוות, וללמד אותם הרגלים נכונים להתנהלות בטוחה בעולם הדיגיטלי של היום

מה הוא הנושא ?

ללמוד להגן על מידע אישי, ליצור סיסמאות חזקות, ולהיות זהירים כשמורידים תוכנות וקבצים הם קריטיים לביטחון הילדים והמידע ששמור על המכשירים הדיגיטליים שלהם. אחרת, ילדים עלולים לחשוף את עצמם ואת משפחותיהם לאיומים דיגיטליים, כמו וירוסים, גניבת מידע וזהות אישיים, ופריצה. בכדי להבין את נושא הבטיחות הדיגיטלית והאבטחה, תצטרכו ללמוד מושגים שעלולים להישמע זרים, כמו: דיוג, נוזקות, תוכנות ריגול, ספאם וזבל. מושגים אלה מתייחסים לתוכנות קטנות וחמדניות שמדביקות את עצמן לתוכנות אחרות, שנראות בטוחות לשימוש – למשל, משחק מחשב שנראה מגניב, אבל ברגע שמתקינים אותו הוא הורס את המחשב. למה זה חשוב? אם ילדים לא יגנו על המידע האישי שלהם הם עלולים להיחשף ולגרום לנזקים פוטנציאלים: נזק לחומרת המחשב, גניבת הזהות הדיגיטלית והפסדים פיננסיים. ילדים אינם מבינים שהם מסכנים את המידע האישי שלהם מאחר וסימני האזהרה לא תמיד בולטים. למשל ילד שמבקש מילד אחר את הסיסמה לטלפון שלו כדי לשחק – ואז נכנס לחשבון המייל שלו מבלי לבקש רשות. או, תוכנה לשיתוף קבצים שילד מוריד למחשב, ועלולה להדביק גם מחשבים אחרים בבית עם וירוס. גנב שמתחזה למישהו אחר עלול לפתות ילדים בבית ספר יסודי לשתף מידע אישי כמו מספר הטלפון בבית, כתובת מגורים, תאריך לידה או מספר תעודת זהות, מהלך שחושף את כל

המשפחה לפגיעה ולגניבת זהות דיגיטלית. כמו בחיים האמיתיים, ילדים שגולשים ברשת חייבים לדעת להבדיל בין אנשים שניתן לבטוח בהם לבין אנשים שלא. למדו אותם:

- לא להשתמש בסיסמאות קלות לניחוש – כמו הכינוי שלהם, או שם החיה שלהם.
- לא להשתמש במידע אישי בסיסמאות שלהם. נוכלים יכולים לעשות שימוש במידע הזה כדי להתחזות אליהם.
- לא להשתמש במילים שקיימות במילון בתור סיסמה – להאקרים יש תוכנות שמנסות את כל המילים במילון כדי לנסות למצוא את הסיסמה הנכונה.
- לעשות שימוש באותיות, ספרות ותווים. סיסמאות אלה קשות יותר לפיצוח ממילים רגילות – מאחר ויש יותר אפשרויות לבניית סיסמה, דבר שיקשה על האקרים לנחש אותה.

חשוב ללמד את הילדים להיות זהירים עם הדברים שהם מורידים. ולהזהיר אותם מהורדה של משחקים חינמיים למחשב, או סרטונים. הקבצים הללו מגיעים לעיתים קרובות עם תוכנות ריגול ווירוסים – שעלולים לגרום לנזק רב. בסופו של דבר, תוכנות שמוצגות כחינמיות לרוב יעלו לבעלים במחיר אחר. חשוב ללמד את הילדים איך לזהות ולהתמודד עם ספאם. ללמד אותם שספאם הוא זבל אינטרנטי. אסור להם לפתוח את ההודעות האלה, אחרת הם יקבלו עוד יותר מהן. האסטרטגיה הטובה ביותר היא לא לפתוח מיילים מכתובות שהם לא מזהים.

**כמה דברים חשובים לגבי סיסמאות**

למרות ההתפתחויות הטכנולוגיות של השנים האחרונות, סיסמאות הן עדיין אמצעי האימות הזמין ביותר לשמירה על החשבונות המקוונים שלנו. למעשה הסיסמה שאנחנו בוחרים היא לפעמים הדבר היחיד שמפריד בין האקרים למידע האישי שלנו ולכן לא כדאי להמעיט בחשיבותן.

בנוסף ליצירה של סיסמאות חזקות חשוב להקפיד על שימוש בסיסמה שונה לכל חשבון – האקרים יודעים שאנחנו מתעצלים ליצור לכל חשבון סיסמה ייחודית, כך שאם הם הצליחו לפרוץ לחשבון אחד סביר להניח שהם יבדקו גם את החשבונות האחרים של אותו משתמש.

## מטרת השיעור

התלמידים יגבירו את רמת האבטחה האישית שלהם ברשת באמצעות זיהוי ויצירת סיסמאות חזקות וקלות לזכירה.

## מטרות הלמידה

- התלמידים יזהו מה הופך סיסמה לחלשה
- התלמידים ידונו במגוון רחב של מאפיינים שתורמים לסיסמה חזקה
- התלמידים יצרו סיסמאות חזקות שקל לזכור בשביל השימוש האישי שלהם באינטרנט, ויפעלו לפי הנהלים הטובים ביותר בנושא הסיסמאות, כדי להבטיח שהאבטחה שלהם ברשת לא נפגעת.

| | |
|---|---|
| **משך הפעילות:** 90 דקות | **מונחים:** סיסמה ייחודית וחזקה, תווים מיוחדים, ביטוי עם משמעות |
| **קהל יעד:** כיתות ד'-ז' | |
| **חומרים**: צ'ק ליסט סיסמאות מושלמות, סרטון אנימציה טיפים לסיסמה חזקה., עלון סייבר מן | |

| | | |
|---|---|---|
| **פתיחה** | דיון בנושא "שיתוף סיסמאות" | 20 דקות |
| **פעילות 1** | סיסמאות מושלמות - שאלות ותשובות | 30 |
| **פעילות 2** | סיעור מוחין בנושא יצירת סיסמאות חזקות | 20 |
| **סיכום** | צ'ק ליסט סיסמאות מושלמות | 10 |

**מהלך הפעילות:**

| | |
|---|---|
| **פתיחה*** <br><br> חשבו על סיבות מדוע אתם צריכים סיסמאות חזקות שאנשים אחרים יתקשו לנחש, ומדוע אתם לא צריכים לחלוק את הסיסמאות שלכם עם אנשים אחרים. | **פעילות (1)** <br><br> עשו סיעור מוחין כקבוצה (או במליאה ) לגבי הדרכים שניתן ליצור באמצעותן סיסמאות חזקות. |
| **פעילות (2)** <br><br> ענו על השאלות של "סיסמאות מושלמות". | **סיכום** <br><br> מלאו את הצ'ק ליסט של סיסמאות מושלמות כדי לראות כמה קריטריונים מילאתם.<br>שנו או החליפו את הסיסמאות הנוכחיות שלכם בשביל רמת אבטחה גבוהה יותר ברשת. |

**<u>מהלך הפעילות</u>:**

א. המורה תפנה לתלמידים ותאמר: מה אתם אוהבים לעשות באמצעות המחשב, הטלפון נייד והטאבלט כשאתם מחוברים לרשת האינטרנט? (מחפשים מידע, משחקים, מסתכלים על תמונות, רואים סרטים, שומעים מוסיקה, שומרים על קשר עם חברים).

1. מדוע אתם צריכים סיסמאות חזקות שאנשים אחרים יתקשו לנחש?
2. המורה תקרין/תכתוב על הלוח את המקרה של בן. ותשאל ומדוע אתם לא צריכים לחלוק את הסיסמאות שלכם עם אנשים אחרים (ראה נספח 1).

*** לשיקול דעת המורה, בשלב זה ניתן להרחיב את הדיון בעזרת אחד משני הסרטונים:**

"מכירים ולומדים ומסכנות ברשת נזהרים"https://www.youtube.com/watch?v=c_M2ORiUXLU

בריינפופ – בטיחות באינטרנט

ב. המורה תלמד את התלמידים את הטריקים ביצירת סיסמה חזקה וייחודית (ראה נספח 2 ).

צפייה במצגת סיסמה חזקה

ג. המורה תקרין/תכתוב על הלוח דוגמאות לתרגול השיטה, ותיתן לתלמידים לעשות סיעור מוחין כקבוצה (או במליאה ) לגבי הדרכים שניתן ליצור באמצעותן סיסמאות חזקות.

ד. המורה תיתן לתלמידים לענות על שאלות של "סיסמאות מושלמות" מצ"ב דף כרטיסיות (נספח 3 ).

**לסיכום** הדיון הכיתתי, המורה תאמר לתלמידים כי ברשת, כמו בחיים האמיתיים, חשוב להבין שההגנה הטובה ביותר נגד תוקפים היא אתה. שמירה על בטיחות ועירנות ולהתייעץ עם מבוגר/לפנות לעזרת מבוגר היא הדרך הטובה ביותר לעזור לעצמך לשאר בטוח.

ה. לסיום השיעור: למלא את הצ'ק ליסט של סיסמה מושלמת (נספח 4).

נספח (1)

בן מגלה לחבר שלו את הסיסמה לפורם הכיתתי. שבוע לאחר מכן הם רבים ובאותו הלילה החבר לשעבר מתחבר בסיסמה של בן. הוא מעמיד פנים שהוא בן ומתנהג בצורה גסה לאנשים שאיתם הוא מדבר. למחרת חבריו של בן לא מדברים איתו כי הם חושבים שהוא זה שדיבר איתם בלילה הקודם.

1) באיזו תדירות אתם משנים את הסיסמה שלכם? באיזו תדירות אתם צריכים לשנות את הסיסמה שלכם?
2) האם כדאי שתהיה לכם את אותה הסיסמה עבור כל חשבון שאתם פותחים באינטרנט?
3) מה עוד יכול לקרות אם אתם משתפים את הסיסמאות שלכם עם חברים?
4) איך אתם יכולים ליצור סיסמאות חזקות שלאחרים יהיה קשה לנחש

נספח(2)

| | |
|---|---|
| | **סיסמה חזקה ומורכבת**<br><br>**חשוב לזכור שסיסמה מורכבת, שלא תיפרץ בקלות, היא סיסמה שמכילה שילוב אקראי של אותיות גדולות וקטנות (באנגלית) ספרות וסימנים. רוב אנשי האבטחה גם ממליצים שהסיסמה תכלול 8 תווים לפחות** |
| | **טריק ראשון - חשבון פשוט**<br><br>טריק אחד ליצור סיסמה שכזו הוא להשתמש בתרגיל חשבון פשוט עם שילוב של מילים במקום ספרות. לדוגמה, הסיסמה 5 Hundred-3=497תהיה סיסמה חזקה למדי שמכילה את כל האלמנטים של סיסמה טובה, היא לא תיפרץ בקלות וגם לא יהיה לכם קשה לזכור אותה. כמובן שאפשר לסבך אותה עוד יותר על ידי שימוש בתרגילים "מורכבים" יותר |
| | **טריק שני - ביטוי עם משמעות**<br><br>טריק נוסף שיעזור לכם ליצור סיסמה חזקה שתזכרו בקלות, תהיה להשתמש בביטוי שיש לו משמעות מבחינתכם. הביטוי חייב להכיל אלמנטים של סיסמה חזקה, אבל צריכה להיות לו משמעות עבורכם כך שתזכרו אותו. לדוגמה (ונניח שיש לי כלב שקוראים לו צ'ובאקה ( ChewbaccaLove 2eat היא סיסמה חזקה מאוד שלא יהיה לי קשה מדיי לזכור. שימו לב שבנוסף לשילוב האותיות הגדולות והקטנות והספרה 2, הסיסמה הזו כוללת גם רווח – דבר שהופך את הסיסמה לחזקה ביותר. |
| | **טריק שלישי - ראשי תיבות**<br><br>ישנו טריק נוסף שבאמצעותו תוכלו ליצור סיסמה חזקה, וזה בעזרת משפט שלם וארוך שיהיה לכם קל לזכור והפיכתו לראשי תיבות. קחו למשל משפט ארוך כמו I used to – ) גרתי פעם בקומה 10 live on the 10th floor on 32 Ben Yehuda street Tel Aviv ברחוב בן יהודה 32 תל אביב) וצרו ממנה את ראשי התיבות הבאים iUtl10f32bYsTLV : והרי לכם סיסמה חזקה שלכל אחד אחר תיראה אקראית לחלוטין, רק תצטרכו לזכור אילו מהאותיות הן "גדולות." |
| | |