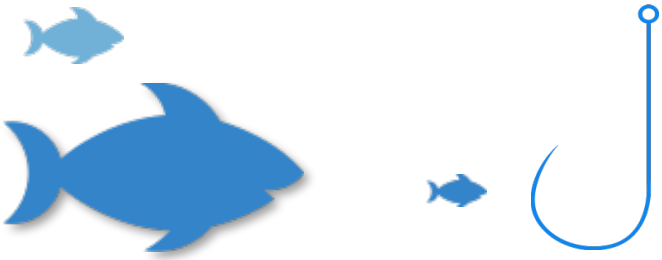
אל תנגסו בקרס הדיג!



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

הקדמה

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 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 האמתיים, ילדים שגולשים ברשת חייבים לדעת להבדיל בין אנשים שניתן לבטוח בהם לבין אנשים שלא.

- 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 וויروסים – 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.

<u>מטרת השיעור</u>

התלמידים יגבירו את רמת האבטחה האישית שלהם ברשת באמצעות משחק שבו הם חוקרים מגוון מיילים וטקסטים, ומנסים להבין אילו מהם מהימנים ואילו מהם הונאות דיוג.

<u>מטרות הלמידה</u>

- ללמוד מה הטכניקות שמשמשות האקרים לגניבת פרטים אישיים
- לחזור על הדרכים בהן ניתן למנוע גניבת מידע אישי.
- לזהות את הסימנים של ניסיונות דיוג
- לדעת לפנות למבוגר אחראי אם הם חושבים שהם הפכו לקורבן של גניבת זהות.
- להיות זהירים לגבי איך ועם מי הם משתפים מידע אישי.

משך הפעילות: 90 דקות
קהל יעד: כיתות ו'-ח'

א. פתיחה - במליאה

המורה תסביר : בואו נדבר מה זה הדיוג הזה, בכל מקרה?

דִּיוּג או פישיינג (באנגלית: Phishing) הוא מצב בו מישהו מנסה לגנוב מידע על חשבון או פרטי ההתחברות באמצעות העמדת פנים של מישהו שאתם סומכים עליו במילים אחרות התחזות לגורם לגיטימי. הוא עושה זאת לרוב באמצעות אימייל, הודעת טקסט, או כל אמצעי תקשורת אינטרנטי אחר. אימיילים של דיוג - והאתרים הלא בטוחים שאליהם הם מנסים לשלוח אתכם, או הקבצים שהם מנסים לגרום לכם להוריד - יכולים גם לשתול וירוסים במחשב שלכם. הווירוסים האלה יכולים לעשות שימוש באנשי הקשר שלכם כדי לפגוע גם בהם. הונאות אחרות יכולות לשכנע אתכם להוריד נוזקות או תוכנות לא רצויות למחשב, בכך שהן מודיעות שיש משהו לא בסדר עם המכשיר שלכם. זכרו: **<u>אתר או פרסומת לא יכולים לדעת אם יש תקלה במכשיר שלכם!.</u>**

חלק מניסיונות הדיוג שקופים למדי, אבל אחרים יכולים להיות מתוחכמים ומשכנעים. למשל, כאשר נוכל שולח לכם הודעה שכוללת בתוכה מידע אישי עליכם, זה נקרא דיוג-חנית ומדובר במהלך מאוד יעיל ומתוחכם. להרחבה

מאוד חשוב לדעת לזהות מוקדם כל דבר מוזר או לא שגרתי במיילים ובטקסטים, לפני שלוחצים על לינקים מפוקפקים או מזינים סיסמאות באתרים מפוקפקים.

<u>הנה כמה שאלות שאפשר לשאול את עצמנו כשאנחנו קוראים הודעה או נכנסים לאתר:</u>

- האם הוא כולל בתוכו אינדיקציות לאתר מהימן, כמו סמלים?
- האם כתובת האתר תואמת את השם והכותרת של מה שאתם מחפשים?
- האם יש באתר הודעות קופצות? (הן לרוב מרמזות שמשהו לא בסדר).
- האם כתובת האתר מתחילה עם "https://" שצבעו ירוק? (המשמעות של הדבר היא שהחיבור מאובטח ומוצפן).
- מה כתוב באותיות הקטנות? (שם הם כותבים את כל הדברים הבעייתיים).

ב. למידה קבוצתית של דוגמאות

המנחה יחלק את הכיתה לקבוצות דיון. כל קבוצה תקבל סיפור מקרה המתאר מקרה של של אירוע התחזות ברשת ומלווה בשאלות לדיון בקבוצה. את התובנות המרכזיות שיעלו בדיון הקבוצתי יציגו התלמידים במליאה. "להלן מספר דוגמאות המתארים אירועים של דיוג והתחזות ברשת . בואו נתחלק לקבוצות, וכל קבוצה תלמד את הדוגמאות האלה להודעות ואתרי דיוג."

- **דיון על הדוגמאות**

-החליטו אילו מן הדוגמאות "אמיתיות" ואילו "מזויפות", וכתבו רשימת סיבות מדוע אתם חושבים כך מתחתיהן

- אילו דוגמאות נראו מהימנות ואילו חשודות? האם היו תשובות שהפתיעו אתכם?

- **שאלות להרחבת הדיון**

-הנה כמה שאלות לשאול את עצמכם כשאתם נתקלים בהודעות ואתרים:

1. האם ההודעה הזאת נראית בטוחה?

2. מה האינסטינקט שלכם אומר? האם אתם נתקלים בחלקים שנראים חשודים?
3. האם המייל מציע לכם משהו בחינם? הצעות חינם בדרך כלל לא באמת חינמיות!

4. האם מבקשים את המידע האישי שלכם?

כמה אתרים מבקשים מידע אישי כדי שיוכלו לשלוח לכם הונאות נוספות. למשל, "מבחני אישיות" יכולים לאסוף עליכם עובדות שיקלו לנחש את הסיסמאות, או מידע אישי אחר שלכם. רוב העסקים האמתיים, מצד שני, לא ישאלו לגבי מידע אישי במייל.

5. האם מדובר במייל משורשר או פוסט חברתי?

מיילים ופוסטים שמבקשים מכם להעביר את ההודעה הלאה לכולם, עלולים לשים אתכם ואת השאר בסכנה. אל תעשו זאת אלא אם אתם בוטחים בשולח, ובכך שהיא בטוחה להעברה הלאה.

6. האם יש אותיות קטנות?

בתחתית המסמך אפשר למצוא את האותיות הקטנות. גודל הטקסט בדרך כלל קטן, ומכיל את כל הדברים שאנחנו אמורים לפספס. למשל, הכותרת הראשית עשויה לומר שזכיתם בטלפון חינם אבל באותיות הקטנות יהיה כתוב שאתם צריכים לשלם לחברה 200 ש"ח בחודש.

ג. דיון במליאה

לאחר העבודה בקבוצות, המורה יזמין נציג/ה מכל קבוצה להציג את התובנות אליהן הגיעו תוך כדי הדיון בסיפור המקרה.

ד. סיכום במליאה

לאחר הדיון בכיתה המורה יסכם ויתייחס לנקודות הבאות:

ומה קורה אם נפלתם קורבן להונאה? קודם כל: אל תילחצו!

- ✓ ספרו מיד להורה, מורה, או מבוגר שאתם בוטחים בו. ככל שתחכו יותר, כך עלולים להתרחש דברים גרועים יותר.
- ✓ שנו את הסיסמאות שלכם עבור החשבונות שברשת.
- ✓ עדכנו והזהירו חברים שעשויים להיפגע כתוצאה מהדיוג.
- ✓ היעזרו בהגדרות כדי לדווח על ההודעה כדואר זבל, במידת האפשר.

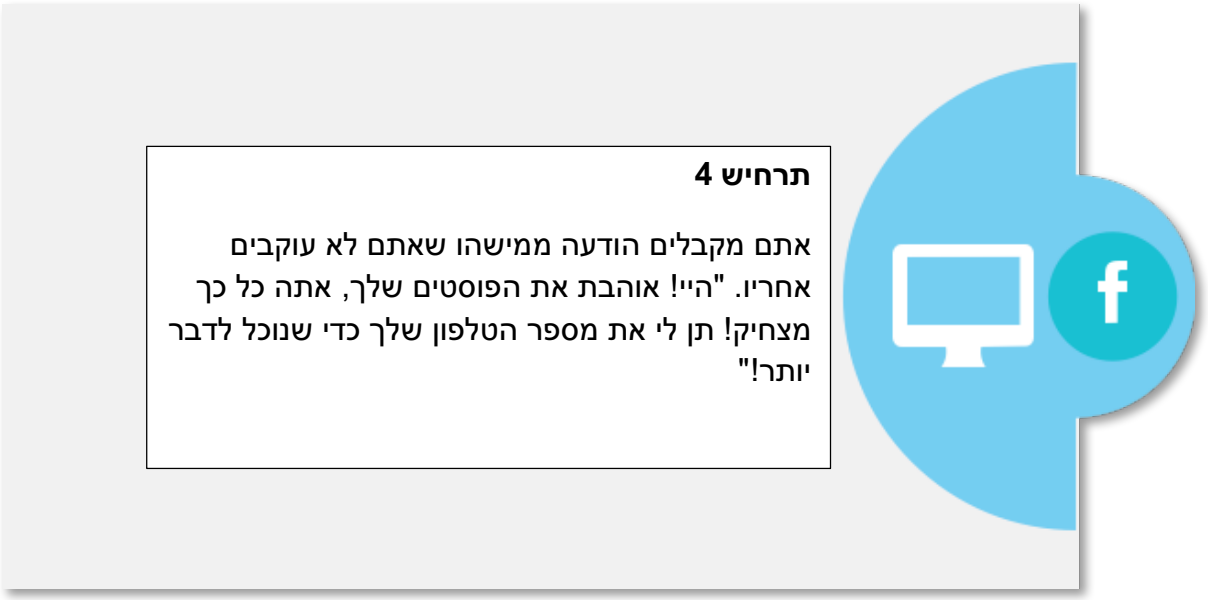
<u>צידה לדרך</u>

כשאתם גולשים ברשת, תמיד עמדו על המשמר לניסיונות דיוג במייל, בהודעות ובפוסטים - ודאגו לעדכן את האנשים הנכונים במקרה ונפלתם קורבן להונאה.

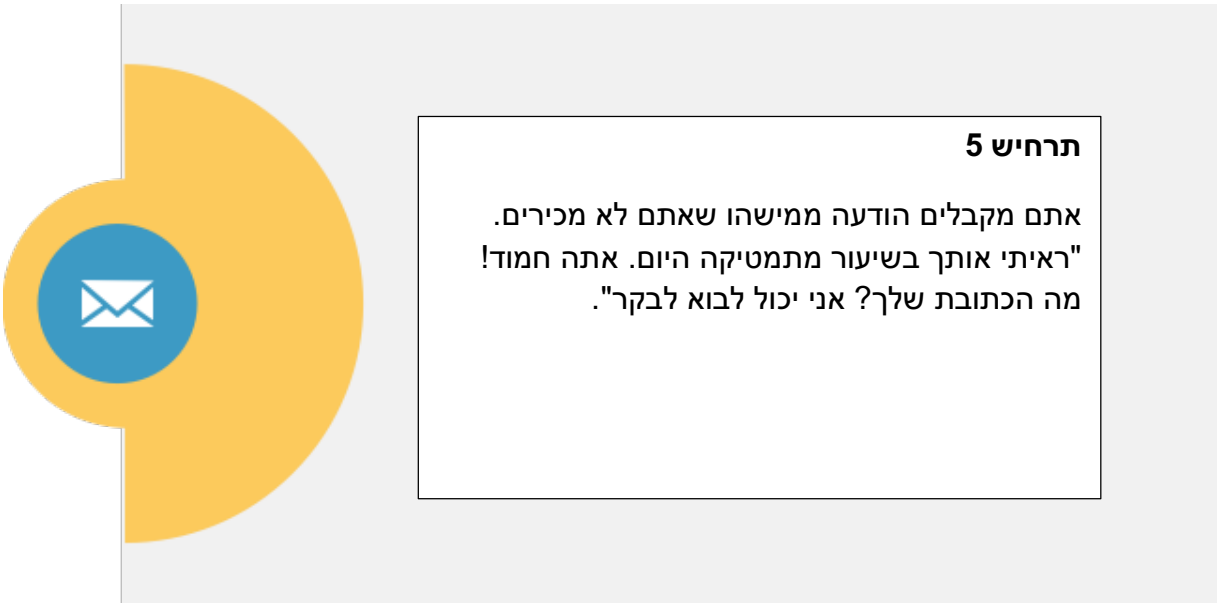
תרחיש 1

אחרי שיעור מתמטיקה עם המורה שלומית, אתם מקבלים הודעה לטלפון. "זה רון משיעור מתמטיקה עם המורה שלומית. הבנת את שיעורי הבית?"

- ☐ **התעלם מרון.** כמו בכל פעם, אם אתם לא מכירים את האדם הזה, אתם לא חייבים להגיב לו כלל.
- ☐ **חסום את רון.** בחירה טובה אם אתם בטוחים שאין שום תלמיד בשם הזה בכיתה.
- ☐ **"היי רון, האם אתה זה שיושב מאחורי?"** אם אתם לא בטוחים, תמיד אפשר לשאול.
- ☐ **"בטח. אני יכול להסביר אחרי בית הספר"** זאת בחירה טובה רק אם אתם בטוחים שאתם מכירים את האדם.
- ☐ **"אני לא לומד עם המורה שלומית - אני לומד אצל המורה שוקי".** אם אתם לא בוטחים באדם הזה בהסתמך על מה שהוא אמר, הבחירה הטובה ביותר שלכם תהיה להתעלם מההודעה. בכל מקרה אתם לא צריכים לתת מידע אישי, כמו שם המורה שלכם.
- ☐ **"תתקשר אליי למספר 052-4445555".** לא מומלץ. אלא אם אתם בטוחים שאתם מכירים את האדם הזה, לא כדאי לשלוח את המידע האישי שלכם.



- ☐ **התעלם מ@אוהבת_כדורגל_12.** אתם לא חייבים להגיב אם אתם לא רוצים.
- ☐ **חסום את @אוהבת_כדורגל_12.** אם האדם נראה חשוד ובחרתם לחסום אותו - לא תשמעו ממנו יותר.
- ☐ **"היי, האם אני מכיר אותך?".** אם אתם לא בטוחים, תשאלו שאלה לפני שאתם מנדבים מידע אישי.
- ☐ **"אוקיי, המספר שלי...".** לא! אפילו אם אתם בטוחים בזהות של השולח, זה לא רעיון טוב לשלוח מידע אישי ברשתות חברתיות. תמצאו דרך אחרת לדבר, דרך ההורים, המורים, או מישהו אחר שאתם בוטחים בו.



- ☐ **התעלם.** כנראה בחירה נבונה.
- ☐ **חסום את האדם הזה.** אל תהסס אם אתה מקבל תחושה רעה לגבי מישהו.
- ☐ **"מי אתה?".** לא כדאי. אם ההודעה נשמעת חשודה, עדיף לא לענות כלל, או לחסום את השולח.
- ☐ **"זאת דנה? את גם חמודה! אני גר בשדרות המלך 4"** זה לא רעיון טוב, למרות שאתם חושבים שאתם מכירים את האדם הזה. לפני שאתם משתפים את הכתובת שבה אתם גרים למישהו חדש, תבררו קצת עליו - גם אם אתם חושבים שאתם מכירים אותו.

תרחיש 6

אתה מקבל את ההודעה הזאת: "היי בדיוק הכרתי את חברה שלך, רעות! היא סיפרה לי לגביך, ואשמח להיפגש איתך! מה הכתובת שלך?"

- **התעלם.** אם אתם לא מכירים את האדם הזה אבל יש לכם חברה בשם רעות, הבחירה הנבונה ביותר תהיה לבדוק עם רעות לפני שתשיבו להודעה.
- **חסום.** אם אתם לא מכירים את האדם הזה ואין לכם חברה בשם רעות, זה כנראה רעיון טוב להיכנס להגדרות ולחסום את איש הקשר הזה מליצור איתכם קשר בהמשך.
- **"מי את?".** כנראה לא הרעיון הטוב ביותר, אם אתם לא מכירים את האדם הזה, עדיף לא לענות, לפחות לא עד ששמעתם מרעות.

- מה זה דיוג
- זיהוי תרמיות והודעות דיוג - אתר מיקרוסופט
- אתר לדיווח על אתרי פישינג
- הסבר על הונאות מקוונות והונאת "פישינג" באתר פרקליטות המדינה