

נושא השיעור

אבטחת מידע והונאות ברשת

שכבת גיל: כיתות ט

ציר מוביל: ציר ראשון – צרכנות מודעת וקבלת החלטות פיננסיות

נושא השיעור:

עוגני השיעור

אבטחת מידע והונאות ברשת: בעולם שבו הכסף שלנו הפך לדיגיטלי, המיומנות הפיננסית הכי חשובה היא

לדעת להגן עליו. ביחידה זו נלמד איך להימנע מהשארת עקבות דיגיטליים ואיך לנווט בביטחון בין אפליקציות תשלום לקניות אונליין, ונחשוף את שיטות ההונאה המתוחכמות ביותר – מהפשינג הקלאסי ועד למלכודות AI שנראות אמיתיות מתמיד. דרך סימולציות של "אמת או זיוף", נלמד לזהות את הנורות האדומות בזמן אמת ולהפוך למשתמשים חכמים ומוגנים במרחב הדיגיטלי.

מושגים מרכזיים:

מערך סייבר, טביעת רגל דיגיטלית, הנדסה חברתית, הונאות בתחפושת, אימות דו שלבי, הרשאות גישה, קובצי קוקיז. סוגי הונאות: פשינג, דיוג קולי, סמישינג, דיפ-פייק, נזקות כופרה (וירוסים), הונאות משלוחים, הונאות ההלוואות, קניה בטוחה ברשת, אתרים מאובטחים, פלטפורמות תשלום בטוחות.

מיומנויות מרכזיות:

אוריינות מידע: התלמידים נדרשים לאסוף מידע, למפות סוגי הונאות בפורמטים ויזואליים ולהעריך את רמת האמינות של מקורות מידע ואתרים.

חשיבה ביקורתית: התלמידים נדרשים לנתח הטיות קוגניטיביות, להטיל ספק במניעי הכותב ולעבד בצורה מטה-קוגניטיבית את תהליכי קבלת ההחלטות שלהם.

אוריינות דיגיטלית: התלמידים נדרשים לבחון כתובות URL ולתפעל פלטפורמות דיגיטליות להצגת נתונים ובדיקת אתרים, הודעות, מיילים וכו' ולדעת איך לנבט ולהיזהר מהשארת עקבות דיגיטליים שמסכנים אותם.

ערכים מרכזיים:

אחריות אישית, יושרה ואמינות, ערכות הדדית, חוסן דיגיטלי, מסוגלות.

משך זמן משוער: (90 דקות)

קישור למצגת המלווה את השיעור: [מצגת אבטחת מידע](#)

שם כותב השיעור: פריאל מסאד

מטרות השיעור:

- מטרה 1: **התלמיד יזהה** "נורות אדומות" ומנגנוני הטעיה בהודעות פשינג ובאתרי מסחר, תוך ניתוח הטיות קוגניטיביות (כמו דחיפות ופחד) ושגיאות לשוניות האופייניות להונאות סייבר.



- מטרה 2: **התלמיד ישווה** בין אתרים ומקורות מידע שונים באמצעות כלי אוריינות דיגיטלית (בדיקת URL, השוואת מחירים וקריאת ביקורות) כדי לקבוע את רמת אמינותם לפני ביצוע פעולה פיננסית.
- מטרה 3: **התלמיד ידגים** מחייו האישיים מקרים של הונאות וידע לאמץ את מה שנלמד על מנת שיוכל להגן על עצמו
- מטרה 4: **התלמיד ינתח** דילמות אתיות ומצבי הונאה באמצעות סימולציות ומשחקי תפקידים, ויגבש מודל פעולה אישי למתן סיוע והסברה לאחרים במקרה של זיהוי פגיעה במרחב הדיגיטלי.

עזרים לשיעור

מצגת, דף עבודה, כרטיסיות בשני צבעים (אדום וירוק), מקרן, רמקול.

[קישור למצגת](#)

מערך שיעור

פתיחה 10 דק: הצגת הנושא וסקר ליצירת עניין בחומר הנלמד
מציגה את הנושאים שנלמד בשיעור של אבטחת מידע והם:

- סייבר וטביעת אצבע דיגיטלית
- סוגי הונאות והנדסה חברתית
- התגוננות מפני הונאות
- קנייה בטוחה ברשת

מטרתה פתיחה: לעורר מודעות לכך שכל פעולה דיגיטלית היא טביעת רגל.
פעילות:

מחלקים לתלמידים כל אחד כרטיסיה אחת ירוקה וכרטיסיה אחת אדומה. מציגה את השקפים מ-3-9 ומבקשת מכל אחד שמסכים עם המשפט או שהאירוע קרה שירים כרטיסיה ירוקה ומי שלא מסכים או שאירוע לא קרה לו שירים כרטיסיה אדומה. תוך כדי אני מבקשת שכל תלמיד יסתכל סביבו ויראה מה המצב הכללי בכיתה.

גוף השיעור:

עקבות דיגיטליים, סוגי הונאות, התגוננות, קניה בטוחה ותשלום מאובטח

אז לפי הרוב המצב יהיה שלרוב התלמידים רוב האירועים במצגת עברו עליהם. פה אני אומרת להם: "מזל טוב, השארת עקבות דיגיטליים" מציגה ומסבירה את המושג "עקבות דיגיטליים": בכל פעם שאתם מתקינים אפליקציה חדשה, קונים בגד ב-Temu או מעבירים קובץ ב-Discord, אתם בעצם משאירים דלת פתוחה. או טביעת אצבע דיגיטלית האם אתם יודעים מי עוד מחזיק במפתח לטלפון, לשעון או לפרטי האשראי שלכם? העקבות הדיגיטליים מכונות גם "טביעת רגל דיגיטלית", ומהוות כלל הנתונים שאדם משאיר אחריו במהלך פעילויותיו המקוונות. עקבות אלו יכולות לכלול אמוג'ים מועדפים, מהירות הקלדה,



צורת התנסחות מגמתית, יישומים מועדפים, תוספים מועדפים, מידע אישי, הרגלי גלישה, אינטראקציות חברתיות ועוד.

ופה אני מציגה איך אנחנו משאירים עקבות דיגיטליים ולכן אני מציגה את שקף 12:
אני מבקשת מהם להסתכל ולגיד לי איך בעצם אנחנו יכולים להשאיר עקבות דיגיטליים. הילדים מתחילים לזרוק תשובות. ואז אני מסכמת את הנושא איך אנו משאירים עקבות דיגיטליים

שקפים 13-16

איך משאירים עקבות דיגיטליים: בואו נכיר ביחד ולפי מה שאתם עניתם ועברתם מהם סוגי העקבות הדיגיטליים

1. רשתות חברתיות:

- תגובות ולייקים - כל תגובה נשמרת עם תאריך וזמן, וניתן להסתיר אך לא למחוק לחלוטין את מניין הלייקים
- תמונות וסטוריז - גם אם נמחקות, ייתכן שנשמרו בשרתים או צולמו במסך על ידי אחרים
- שיתוף/הפצה - העתקת תוכן וחיפוש שלו יוצרים "עקבות" מרובים ברשת, שקשה למחוק לגמרי ברגע שהתוכן הופץ

2. משחקי רשת וצ'אטים:

- הודעות בקבוצות וואטסאפ - נשמרות אצל כל משתתפי הקבוצה
- שיחות בדיסקורד - מתועדות בשרתים ובלוגים
- אינטראקציות במשחקי וידאו מקוונים - נשמרות בהיסטוריית המשחק ולעיתים משודרות בשידור חי

3. היסטוריה של חיפוש:

- חיפוש גוגל
- היסטוריית צפייה ביוטיוב
- זמן הצפייה בסרטונים - אלגוריתמים לומדים דפוסי התנהגות (אמוג'ים מועדפים, הרגלי גלישה) כדי להתאים פרסומות אישיות

4. נתוני מיקום GPS

- נתוני מיקום GPS
- אפליקציות מפות
- תיוג מיקום ברשתות חברתיות
- אפליקציות מזג אוויר/ספורט - עוקבות ברקע גם ללא מודעות מלאה של המשתמש

סוגי הונאות ברשת:

כפי שאמרנו בגלישה ובפעולות השונות שאנו עושים אנו משאירים עקבות וטביעת רגל דיגיטלית אשר מאפשרת לאנשים זרים להשתמש במידע שהשארנו בדרך לא אתית.

סוג 1: הנדסה חברתית (שקף 17):



הנדסה חברתית (Social Engineering) היא טכניקה של מניפולציה פסיכולוגית המשמשת כדי לגרום לאנשים לבצע פעולות או לחשוף מידע סודי. בניגוד לתקיפות סייבר "רגילות" המבוססות על פרצות בתוכנה או בקוד, הנדסה חברתית מנצלת את "החוליה החלשה" ביותר בשרשרת האבטחה: הגורם האנושי.

הנדסה חברתית עובדת בשלבים:

שלב 1: איסוף מידע: התוקף חוקר את הקורבן (דרך רשתות חברתיות, אתרי חברה וכו') כדי למצוא נקודות תורפה.

שלב 2: יצירת קשר: פנייה לקורבן תוך שימוש בזהות בדויה (למשל: נציג תמיכה טכנית, מנהל בבנק או קולגה).

שלב 3: המניפולציה: שימוש בסיפור כיסוי (Pretexting) כדי להוציא מידע או לגרום לפעולה.

שלב 4: ביצוע המשימה: הקורבן מעביר את הסיסמה, לוחץ על הקישור או מבצע את ההעברה הכספית.

אז בואו נקח דוגמה ונבין איך זה בדיוק קורה: (שקף 18):

נועה היא ילדה בכיתה ט. נוכל עוקב אחרי הסטוריז שלה ואז הוא שם לב שהיא עוקבת אחרי זמר שלפי הפעילות שלה (לייקים, שיתופים, תגובות...) - אפרופו עקבות דיגיטליים היא שרופה עליו. זהו שלב של ... "איסוף מידע". אז הוא שולח לה הודעה שבה הוא הודיע לה על זכייה בכרטיסים להופעה, ההטבה מוגבלת עד לזמן מסוים. זהו שלב יצירת הקשר. נועה התלהבה מאוד ואמרה לעצמה: "ברור שאני רוצה, כל כך חיכיתי לזה" וכמובן היא נכנסה לקישור בהודעה שהי קיבלה מהנוכל. זהו שלב ... מניפולציה. ואז במשך התבליך הסתבר שהיא צריכה לשים את פרטי כרטיס האשראי של ההורים כדי לממש את הזכייה. כמובן שנעה כמעט "ביצעה את המשימה" ומסרה את הפרטי האשראי אבל לשמחתינו היא נזכרה בשיעור של הונאות פיננסיות שהיא למדה.

סוגי שני של הונאות זה-ה-דיוג / PHISHING שקף 19

פשינג או דיוג הוא ניסיון לגנוב מידע אישי כמו שם משתמש, סיסמאות, כרטיסי אשראי ועוד, ולגרום לנו ללחוץ על קישורים זדוניים (המובילים להונאה).

יש כמה סוגים של דיוג:

1. דיוג קולי: - התוקפים מתחזים לגופים מוכרים, כגון: בנקים, משרדי ממשלה, ומנסים לגרום לקורבן לחשוף מידע אישי ולבצע פעולות מסוימות דרך הטלפון.

מי יכול לשתף אותנו במקרה כזה ?

מה עושים במצב כזה ?

מה שנכון לעשות על מנת לא לפספס הזדמנות או שיחה חשובה זה כדאי לבקש מספר טלפון, ולבקש לנתק את השיחה ואתם תתקשרו לוודא שהם אכן שייכים לארגון שממנו הוא הציג את עצמו.



2. דיג ממוקד: התוקפים אוספים מידע ממוקד מפעילות של הקורבנות ברשת. הם מתחזים לאנשים בעלי תחומי עניין דומים וגורמים לקורבנות להאמין שמדובר בגורם אמין. אז מה כדאי לעשות?
3. דיג באמצעות הודעה SMISHING. מקבלים לא מעט הודעות (ואם מישהו בסקר שיתף על דבר כזה אפשר גם להוסיף ולקשר את השיתופים שהיו בסקר עם החומר הזה). אם מקבלים הודעה לטלפון או למייל בשום פנים ואופן לא ללחוץ על הקישור. מה שעושים מחפשים אמצעי קשר ואתם פונים לארגון שפנה אליכם, כך אפשר לוודא שההודעה אמינה.
4. דיפ פייק: התוקפים משתמשים בתוכנות בינה מלאכותית ומתחזים לאנשים, כגון: מנכ"לים, מפורסמים, חברים וכדו'.
למשל מקליטים קול של מישהו ואז משתמשים בהקלטה זו ומדברים בקול זה עם אחד מקרובי המשפחה, לרוב קשישים ומבקשים מהם כסף או פרטי כרטיסי אשראי וכו'.
כולנו יודעים שעם החידושים הטכנולוגיים נוכלים מפתחים עוד ועוד שיטות איך לרמות ואנו צריכים להיות זהירים.
5. התחזות ברשתות החברתיות: התוקפים מתחזים ברשתות החברתיות ומבקשים מידע אישי תחת אשליה שמדובר בגורם לגיטימי. לדוגמה: עמודים המתחזים לאינסטגרם ומתריעים כי "חשבונך יושבת", מתחזים לאתר ממשלתי וכדו'.
ההתחזות ברשתות חברתיות היא תופעה שהולכת ומקבלת תאוצה ויש לא מעט אנשים שנפלו בה. ישנם לא מעט נוכלים שמקבלים עלינו מידע דרך הרשתות החברתיות. כדי להגם על עצמינו כדאי להימנע מלהוסיף כחברים אנשים שנראים חשודים, אנשים שאין בינינו לביניהם חברים משותפים, שהשם שלהם נראה מוזר. בדרך כלל אלה מהווים סכנה רצינית

אז בואו נקח כמה דוגמאות להמחיש את מה שנלמד:

דוגמא 1 - פשינג משלוחים:

זוהי הונאה נפוצה מאוד בזמן האחרון. הם משתמשים בה כי הסבירות שאנשים שמקבלים את ההודעה יפלו בהונאה מאוד גבוהה היות והיא נראת הודעה סבירה מאוד.

איך תדעו אם ההודעה שקיבלתם מחברת המשלוחים אמיתית או שמנסים לדג אתכם?

1. יצירת לחץ ותחושת דחיפות – בקשה לביצוע פעולות מידיות מתוך "דחיפות", היא טכניקה נפוצה שנועדה לגרום לאנשים לפעול מלחץ ולהטעות אותם.
2. היעדר פניה אישית – לרוב, ארגונים רשמיים משתמשים בשם הפרטי של הלקוח ופונים אליו באופן אישי. פנייה כללית של "לקוח יקר", עשויה להוות סימן מחשיד.
3. הפנייה לאתרים חיצוניים – אתרים מתחזים, עלולים להיראות דומים מאוד בנראות האתר והדומיין למקור, ולכן מומלץ להיכנס לאתר דרך הדפדפן ולא ללחוץ על הקישור.
4. הצלבת מידע קצרה – אם התקבלה הודעה על תשלום על חבילה שהוזמנה, מומלץ להצליב את מספר ההזמנה שמופיע בהודעה, עם אישור ההזמנה שהתקבל בעת הרכישה. אפשרות



אחרת היא לבדוק באתר הרשמי של דואר ישראל או באפליקציית הדואר החדשה באזור מעקב המשלוחים על ידי הקלדת מספר פריט האם החבילה שהוזמנה הגיעה.

5. לא מוסרים מידע – קיבלתם הודעה מוזרה, או הודעה שנראית לגיטימית אשר לשם ביטולה אתם נדרשים לתת קוד אימות או את פרטי כרטיס האשראי שלכם- עצרו! היו ערניים לבקשות למסירת פרטים אישיים, קודים וסיסמאות.

דוגמה 2: פשינג הלוואות

לא מעט אנשים לאחרונה מקבלים הודעה על אפשרות לקבלת הלוואה בתנאים טובים

חובה לציין שכם תנאים טובים מדי הם סיבה טובה שמעוררת ספר באמינות שלה.

זה נחשה סמישינג אבל גם דיוג ממוקד. כי הנוכלים יש להם לפעמים גישה למידע עלינו מתוך הגלישה והם יודעים מי מהציבור נמצא במצוקה כלכלית, כך שאם הם יקבלו הודעה כזאת יש סיכוי שהם יתפתו להצעה וילחצו על הקישור על מנת לכנס ולבדוק. במקרה ולחצי זה אומר שמסרנו את המפתחות שלנו לאנשים זרים והם יכולים לכנס למרחב הפרטי שלנו שהוא כבר לא מוגן.

מה שהכון לעשות זה להתעלם מהודעות האלה, ברור גם לא לכנס קישורים בשום פנים ואופן.

דוגמה 3: פשינג כביש שש

זו גם הודעה נפוצה שלא מעט אנשים קיבלו אותה והסתבר שהיא הייתה הונאה

דוגמה 4: פשינג קשישים

קשישים הם שכבת גיל שקל מאוד להפיל אותם בהונאה וזה מה היה בשנים האחרונות:

אחרי שמסבירים את ההודעה אני שואלת את התלמידים מהם סימני הזהיו לכך שההודעה היא הונאה?

1. התחזות לגורמים רשמיים: נוכלים מתחזים לעיתים קרובות לנציגי ביטוח לאומי, אנשי משטרה, נציגי מכירות, חברות המספקות שירותי חירום רפואיים (המתחזים לרופאים), ואף משתמשים ב"שיחות שירות" כדי לרכוש את אמון הקשישים ולהוציא מהם כספים
2. מיקוד באוכלוסיות ספציפיות: קיימת תופעה מוכרת של "עוקץ רוסי" המכוונת כלפי קשישים יוצאי מדינות ברית המועצות לשעבר. המשטרה קיבלה למעלה מ-400 תלונות בנושא, ומתחילת שנת 2026 הוגשו 171 כתבי אישום בתיקי מרמה נגד אוכלוסייה זו
3. היקף כספי ורשתות מאורגנות: מדובר בהונאות שגובות מקורבנותיהן סכומי ענק המגיעים למיליוני שקלים, כגון מקרה בו חוליה של 11 חשודים עקצה קשישים בכמיליון שקל, או קשישה בת 92 שנעקצה בעשרות אלפי שקלים.

סוג 3: הונאות בתחפושת (שקף 25)



הונאות מסתתרות מאחורי ניסיונות פיתוי לקנייה שנתפסים כאטרקטיביים. לדוגמה:

הצעת מחיר זולה במיוחד,

הטבה אטרקטיבית מאוד לזמן מוגבל.

הונאות מסתתרות גם מאחורי הבטחה לרגשות נעימים. לדוגמה: חיבור, שייכות, ניראות, הכרה, הוקרה, מעמד.

הונאה סוד 4: שקף 26

כופרה (Ransomware) היא תוכנה זדונית (נוזקה) נפוצה מאוד, אשר נועדה לסחוט כסף מקורבנות ברשת

ההונאה עובדת לרוב בשלבים הבאים:

שלב 1: חדירה למערכת: התוכנה מדביקה מכשיר סלולרי, מחשב אישי או רשת מחשבים שלמה

שלב 2: הצפנה ונעילה: הנוזקה נועלת את הגישה למערכת או מצפינה את כל המידע והקבצים החשובים שמאוחסנים בה. תהליך זה מתבצע לעיתים תוך שימוש במפתחות הצפנה ובחיבור לשרתי שליטה מרחוק של התוקפים

שלב 3: סחיטת דמי כופר: התוקפים דורשים מהקורבן לשלם סכום כסף (לרוב במטבעות וירטואליים קשים למעקב), ובתמורה מבטיחים להסיר את מגבלת הגישה ולשחרר את הקבצים

אחרי הכרנו את סוגי ההונאות בואו נראה מה באמת הכי נפוצים ומה פחות נפוצים. אבל קודם אני מבקשת מהם שינחשו איזה הונאה לדעתם הכי נפוצה. אז אני מבקשת שידרגו את ההונאות מהנפוץ ביותר לחות נפוץ. ואז אני מציגה את השקף הבא:

שקף 27 : סטטיסטיקה, היקף סוגי ההונאות השונים בארץ

- פשינג SMS הן מהוות 35% ממקרי ההונאות המדווחים ולרוב "מחכה לך חבילה" או "חשבוך נחסם"
- פריצה לרשתות חברתיות 25% מסך ההונאות - השתלטות על האינסטגרם
- הונאות צרכניות AI או דיפ פייק 20% בעיקר זיוף של אתרי קניות
- וירוסים וכופרה 20%

שקף 28: השאלה איך נוכל לזהות שמדובר בהונאה? יש לשים לב ולבדוק את האלמנטים הבאים:

1. האם השיחה הגיונית?
2. האם יש בה אלמנט לחץ ודחיפות?
3. האם יש בה פניה אישית?



4. האם ציפינו לקבל שיחה או הודעה זו?

כדי לתרגל זיהוי הודעות בואו נתרגל:

מתן קיבל שיחת טלפון:

"שלום מתן, אני מדבר ממוקד השירות של הבנק. זיהינו פעילות חשודה וחריגה בחשבון שלך לאחרונה, כדי למנוע את חסימת החשבון או גניבת הכספים, אנחנו חייבים לאמת את פרטי ההזדהות שלך כעת ולהעביר קוד אימות שקיבלת לסלולר. אנא מסר לי מיד את הקוד כדי שנוכל לבטל את החסימה.

מה נראה לכם חשוד בהודעה זו? אני נותנת לתלמידים זמן להסכתל, לבחון ולחשוב על השיחה שמתן קיבל מהפיק בבנק.

באמת השיחה חשודה. יש בה כל האלנמטים שמעוררים חשש.

מה הייתם ממליצים ללמתן לעשות?

נקח עוד דוגמא:

שקף 30 - דוגמא להודעה חשודה

"שלום אלה, יש לך חוב פתוח בכביש 6 בסך 47.90 ש"ח שעליך לשלם בתוך 24 שעות כדי למנוע צבירת ריביות. עקב אי-תשלום, התיק הועבר לטיפול משפטי מזורז.

לצפייה בפרטים ולתשלום מהיר היכנסו לקישור הבא: לחץ על הקישור

מסקשת מהתלמידים להתבונן בהודעה ולכתוב מה דעתם? ומה בהודעה מעורר חשד שהיא הונאה.

אכן האלטים של דחיפות ולחץ, ההודעה מאוד בגיונית, יש פניה אישית וכל זה גורם לי להיזהר ולא ללחוץ על הקישור.

פירמידת הגילאים של הונאות:

יופי ראינו מהסקר שעשינו וחלק מכם שיתף מהנסיון שלנו וכמעט כולנו פה ושם השאירו טביעת רגל דיגיטלית. ולא מעט מאיתנו עברו או שמעו מקרוב על הונאה ובמיוחד בקרב צעירים.

רוצה לשאול אותכם לגבי פירמידת הגילאים ואיפה אתם בני נוער נמצאים בהקשר של הונאות?

בני נוער נמצאים לא מעט ברשתות ובאינטרנט ובכל מקום



הסתבר לפי הסטטיסטיקה שצעירים מתחת לגיל 35 (בנוסף לקשישים שדיברנו עליהם לפני) נוטים לספק בקלות רבה יותר מידע אישי ופיננסי ברשת.

השאלה למה לדעתכם (אני אשמע את התלמידים ואז אציג את התשובות בשקף).

אני מעלה את המצגת ומראה להם את הסיבות ומבקשת מהם שוב בהצבעה לציין האם זה נכון במידה מסוימת עבורם.

אז מצבכם כמו מצבם של בני גילאים שלכם השאלה מה זה טביעת / עקבות דיגיטליים שאנחנו משאירים בזמן שאנחנו מבצעים את הפעולות

מה שמאפיין את בני גילכם זה: חוסר נסיון, אימון באמצעים טכנולוגיים, נטיב להתנהגות אימפולסיבית, חוסר ידע ורצון להצלחה כלכלית מהירה.

השאלה לדעתכם האם אפשר למנוע הונאות ברשת?

התשובה היא כן ובואו נראה את הכללים (שקף 33)

1. סיסמה חזקה

כלל 1 : השתמשו בסיסמה ארוכה המכילה כ-12 תווים המורכבת מאותיות גדולות, קטנות, מספרים ותווים מיוחדים

כלל 2: הימנעו משימוש בסיסמאות נפוצות, כגון: תאריך לידה, מספרים עוקבים, כתובת מייל

כלל 3 : מיצאו דרך יצירתית לזכירת הסיסמה, לדוגמה: פזמון משיר אהוב

כלל 4: כדאי להשתמש בתוכנה מאובטחת לניהול סיסמאות, ולהגדיר עבור ההתחברות אליה סיסמה חזקה, לשנות סיסמה באופן קבוע. ולהגדיר לתוכנת ניהול הסיסמאות אימות דו-שלבי.

2. נמנעים משיתוף יתר : על מנת להפחית בהשארת עקבות דיגיטליים

3. הגדרת פרטיות – ואימות דו שלבי

4. לא מאשרים חברות ברשתות חברתיות אם אין חברים משותפים – לבדוק קודם כשמורידים אפליקציה לא מאשרים כל הרשאה אלא רק הרשאות הכרחיות ובזמן שימוש באפליקציה בלבד



סיכום ביניים:

אחרי שלמדנו מה זה טביעת רגל דיגיטלית, מהם סוגי ההונאות, וראינו דוגמאות בואו נבחן את עצמינו בשאלות

שאלות להפעלה בכיתה : שקפים 34-39

מבדק להערכת קשב והבנה

קניה בטוחה באינטרנט: שקף 40

אחרי שלמדנו מה זה טביעת אצבע דיגיטלית ואיך שאנו משאירים מידע עלינו בגלישה באינטרנט ולמדנו גם איך אנשים משתמשים במידע זה כדי לעשות הונאות ומה הם סוגי ההונאות יש לעבור עכשיו למה שהכי חשוב וזה הכיס שלנו.

לא מעט אנשין היום התרגלו לקניה באינטרנט אך זה מעלה את הסיכויים שלנו לעבור הונאה היות שבקניה אנו מספקים מידע רגיש לרבות אמצעי תשלום

קודם בואו נסתובב ונקבע פגישות, נשוחח ונשמע סיפורים מחברינו בכיתה.

ההפעלה : מחלקים שעון פגישות לתלמידים :

[קישור לשעון פגישות](#)

<https://drive.google.com/file/d/1imDD-QGD8trDew4Gt0biNUdad7ELmvMR/view?usp=sharing>

מבקשת מהתלמידים להסתובב ולקבוע פגישות עם 5 תלמידים בכיתה

אני משתמשת בפעמון, מציינת שעה מסוימת. מי שקבע פגישה באותה שעה נפגשים ביחד ונותנים להם סוגיה לדיון ושיחה ביניהם לפי הסדר .

השאלות כתובות במצגת:

1. מה אומר לכם המושג "קנייה בטוחה ברשת"?
2. מה יכולות להיות ההשלכות של קניה "לא" בטוחה ברשת?
3. כיצד תוכלו לוודא שאתם מבצעים קניה בטוחה ברשת?
4. איזה אמצעי תשלום אתם משתמשים בקניה באינטרנט?
5. מהו הדבר הכי קשה שקרה לך/ לאחד מהמשפחה בתהליך קניה באינטרנט

קניה בטוחה באינטרנט: אתרים מאובטחים שקפים 45-51

איך אפשר לזהות שהאתרים שגולשים בהם הם אתרים מאובטחים:

1. ליד הכתובת אתר מאובטח מסומן על ידי מנעול סגור, וכתובת האתר מסתיימת באותיות https (ולא HTTP לבד)
2. אתר אמין מסתיים בסיומת com או co.il
3. מומלץ לגלוש רק דרך רשת Wifi פרטית מאובטחת או דרך Wifi ציבורי במקומות מוכרים (לדוגמה)
4. שגיאות כתיב – ניסוח לקוי או עם שגיאות כתיב יכול להעיד כי מדובר באתר מתחזה. שימו לב לנוסחים המופיעים באתר ושימו לב לשגיאות וליקויים.
5. סקירות וחוות דעת – מומלץ לבדוק אם יש ברשת סקירות או חוות דעת על האתר והאם יש לאתר עמוד פעיל ברשתות החברתיות.
6. פרטים מזהים – חפשו באתר את פרטי ההתקשרות עם החברה ב"אודות" או ב"צור קשר" וכתובת.
7. הגעה ישירה לאתר ולא באמצעות קישורים – עדיף לגלוש באתרים דרך חיפוש בלתי תלוי בגוגל ולא דרך קישורים או מהקלקה ישירה.

הכי חשוב זה הכיס שלנו – אז יש לשים לב איזה פלטפורמה טובה לתשלום באינטרנט:

שקף 52 - קניה בטוחה באינטנט - תשלום מאובטח

אני שומעת 4-5 תלמידים איך הם משלמים ואז אני מציגה ומסכמת את האמצעי תשלום המומלצים לתשלום באינטרנט:

1. הזדהות חכמה – בכל שירות בו הוזנו פרטי האשראי, או בעת שימוש בארנק דיגיטלי, מומלץ לוודא הפעלת הזדהות בטוחה באמצעות קוד אישי חד פעמי בטרם ביצוע עסקה. את ההזדהות הבטוחה ניתן להפעיל באמצעות חברות האשראי פייס ID
2. כרטיס אשראי נטען – בו אפשר לטעון סכום מוגבל. מונע את חשיפת חשבון הבנק להונאות ובמקרה של דלף מספר הכרטיס, מגביל את היקף הפגיעה.
3. פלטפורמות תשלום מקוונות – הנתונים המאוחסנים בפלטפורמות תשלום מקוונות מוצפנים ולא מועברים למוכר בעת התשלום. מומלץ להשתמש בפלטפורמות מסוג זה, כגון PayPal, Google Pay, Apple Pay ו-Bit-i דומיהם, תוך שימוש באימות של קוד, טביעת אצבע או זיהוי פנים, על פני הקלדת פרטי כרטיס האשראי ישירות באתר.

4. תקן PCI DSS – תקן שנקבע על ידי חברות כרטיסי האשראי הגדולות כדי להבטיח הגנה על נתוני כרטיס האשראי בכל מקום בו הם מאוחסנים. בשלב הרכישה באתר מומלץ לבדוק אם מופיע סימן תקן Pci dss של חברות האשראי שבדרך כלל יופיע במסך הרכישה בשולי הדף.

לסיכום אם נפלתם בהונאה לא להתבייש לשתף את ההורים, או מי שאנם סוכמים עליו כדי לעצור את הנזקים

שקף 53 – קישורים לאתרים לבקשת עזרה

מידע נוסף להעשרה והרחבת הידע למורה

[סביבת סייבר לחטיבת ביניים](#)

[מערך הסייבר הלאומי](#)

העשרה למורה

הרחבה והעמקה של נושאים למורה או חומר עזר רלוונטי לשיעור

קישורים רלוונטיים

[סביבת סייבר לחטיבת ביניים](#)

[מערך הסייבר הלאומי](#)

[אתר טעימות פינגסיות](#)

צידה לדרך- נספחים

[קישור דף עבודה 1](#)

[קישור דף עבודה 2](#)

[קישור שעון פגישות](#)



בוחן מסכם יחידה

