כיתה ט' | חינוך פיננסי | שיעור 6 מתוך 14 | 45 דק' | מתאים לממלכתי וממלכתי-דתי

🔒 הונאות ברשת ושמירה על המידע

🎯 מטרות השיעור

- לזהות סימנים של הודעות הונאה (דיוג) במייל, בהודעות ובטלפון
- להכיר הרגלים שמגינים על חשבונות ועל כסף
- לדעת למי פונים כשנפלו בהונאה

🚪 פתק כניסה (2 דקות)

בתחילת השיעור כל תלמיד עונה על פתק, בלי ציון:

1. קיבלתם פעם הודעה מוזרה עם קישור (חבילה, פרס, חשבון חסום)? מה היה כתוב בה?
2. כמה מהחשבונות שלכם משתמשים באותה סיסמה? (רק לעצמכם, לא לשתף)
3. למי מותר לתת קוד שקיבלתם ב-SMS?

למורה: 1. אוספים דוגמאות בלי שמות ובלי מספרים אמיתיים. 2. השאלה אישית ונשארת אצל התלמיד; היא מכינה את הדיון על סיסמה שונה לכל חשבון. 3. התשובה: לאף אחד. זה המסר המרכזי של השיעור. אין צורך לתקן עכשיו; הפתקים מראים למורה מה התלמידים כבר יודעים.

🔑 מושגי מפתח

דיוג (פישינג)
ניסיון להוציא מאיתנו סיסמה, קוד או פרטי תשלום בעזרת הודעה שמתחזה לגוף אמין.

הנדסה חברתית
שימוש בלחץ, בפחד או בסקרנות כדי לגרום לנו לפעול בלי לחשוב.

אימות דו־שלבי
שכבת הגנה נוספת: מלבד הסיסמה צריך גם קוד חד־פעמי.

טביעת רגל דיגיטלית
כל המידע שאנחנו משאירים ברשת, שאפשר לאסוף עלינו.

📖 הסבר למורה

הונאות ברשת כמעט תמיד בנויות אותו דבר: הודעה שנראית רשמית (חבילה שמחכה, חשבון שנחסם, פרס שזכיתם בו), לחץ זמן ('תוך שעה!'), וקישור או בקשה למסור קוד. המטרה היא לגרום לנו לפעול מהר

לפני שנחשוב.

ההגנה הטובה היא הרגלים: לא ללחוץ על קישורים בהודעות לא צפויות, להיכנס לאתר ישירות ולא דרך הקישור, לא למסור לאף אחד קוד שהגיע ב-SMS, להפעיל אימות דו־שלבי, ולבחור סיסמאות שונות לחשבונות שונים. מי שנפל בהונאה צריך לפעול מהר: לשנות סיסמאות, להודיע להורים ולחברת האשראי או לבנק, ולפנות למוקד 119 של מערך הסייבר הלאומי.

👩‍🏫 פעילות בכיתה

1. פתק כניסה (2 דקות): התלמידים עונים על שלוש שאלות קצרות (ראו למעלה).
2. פתיחה: המורה מקרינה 4 הודעות דמיוניות שהיא כותבת מראש (שתיים אמינות ושתיים מזויפות). התלמידים מצביעים: אמיתית או מזויפת?
3. דיון: מה הסגיר את ההודעות המזויפות? בונים על הלוח רשימת 'נורות אדומות'.
4. בזוגות: כל זוג כותב הודעת הונאה דמיונית, וזוג אחר מנסה לזהות בה את הנורות האדומות.
5. מילוי דף העבודה.
6. כרטיס יציאה (2 דקות). מי שסיים מוקדם: ★ חלק אקסטרה למתקדמים בדף העבודה.

💡 הערות למורה

לא להשתמש בשמות של חברות אמיתיות בהודעות לדוגמה. כדאי לעודד תלמידים לשתף בבית את מה שלמדו, כי גם מבוגרים נופלים בהונאות.

❓ שאלות תרגול (בודקים בלחיצה)

1. מה המטרה של לחץ זמן בהודעת הונאה?

לעזור לנו | לגרום לנו לפעול בלי לחשוב | לחסוך לנו זמן | אין לו מטרה

2. מה הדרך הבטוחה להיכנס לחשבון אחרי הודעה חשודה?

דרך הקישור בהודעה | ישירות דרך האתר או האפליקציה הרשמיים | דרך קישור שחבר שלח | אף פעם לא להיכנס

3. למי אפשר לפנות בישראל בנושא הונאה ברשת?

מוקד 119 של מערך הסייבר הלאומי | אף אחד | רק לחברים | לשולח ההודעה

🎟️ כרטיס יציאה (2 דקות)

בסוף השיעור כל תלמיד כותב על פתק:

1. כתבו שתי נורות אדומות בהודעת הונאה.
2. מה תעשו אם לחצתם בטעות על קישור חשוד ומסרתם סיסמה?

תשובות אפשריות: 1. למשל: לחץ זמן, קישור מוזר, שגיאות כתיב, בקשה לקוד או לפרטי אשראי, פרס שלא השתתפתם בשבילו. 2. לשנות סיסמה מיד (ובכל מקום שבו השתמשתם בה), להפעיל אימות דו־שלבי, לספר להורים; אם נמסרו פרטי תשלום, לפנות לבנק או לחברת האשראי ולמוקד 119.

📝 בדף העבודה

פתק כניסה, 5 תרגילים, ★ חלק אקסטרה למתקדמים וכרטיס יציאה. מחוון מלא בעמוד השני. למתקשים יש דף עם תמיכה: מחסן מילים, שאלות הקפה ומשפטי פתיחה.

המידע כללי ואינו ייעוץ פיננסי או משפטי מותאם אישית. כל המספרים והשמות בשיעור דמיוניים.

מחוון: הונאות ברשת ושמירה על המידע

🚪 **פתק כניסה:** 1. אוספים דוגמאות בלי שמות ובלי מספרים אמיתיים. 2. השאלה אישית ונשארת אצל התלמיד; היא מכינה את הדיון על סיסמה שונה לכל חשבון. 3. התשובה: לאף אחד. זה המסר המרכזי של השיעור. לקבל כל תשובה סבירה; הפתק לא נבדק בציון.

1. ב. לא ללחוץ, ולבדוק ישירות באתר או מול השולח
2. ב. לא מוסרים קוד לאף אחד ומנתקים
3. למשל: לחץ זמן, קישור מוזר, שגיאות כתיב, בקשה לקוד או לפרטי אשראי, פרס שלא השתתפתם בשבילו.
4. מלבד סיסמה צריך גם קוד חד־פעמי, ולכן מי שגנב רק את הסיסמה לא יכול להיכנס.
5. לשנות סיסמה מיד (ובכל מקום שבו השתמש בה), להפעיל אימות דו־שלבי, לספר להורים, ואם נמסרו פרטי תשלום, לפנות לחברת האשראי או לבנק ולמוקד 119.

★ חלק אקסטרה למתקדמים

6. לבדוק שההודעה הדמיונית כוללת סימנים כמו לחץ זמן, קישור מקוצר או משונה, בקשה לקוד. ההודעה האמיתית: בלי קישור לתשלום, מפנה לאתר או לאפליקציה הרשמיים, בלי לחץ.
7. כשסיסמה דולפת מאתר אחד, מנסים אותה גם באתרים אחרים. סיסמה שונה לכל חשבון מגבילה את הנזק לחשבון אחד.

🎟️ **כרטיס יציאה:** 1. למשל: לחץ זמן, קישור מוזר, שגיאות כתיב, בקשה לקוד או לפרטי אשראי, פרס שלא השתתפתם בשבילו. 2. לשנות סיסמה מיד (ובכל מקום שבו השתמשתם בה), להפעיל אימות דו־שלבי, לספר להורים; אם נמסרו פרטי תשלום, לפנות לבנק או לחברת האשראי ולמוקד 119.

נכתב על ידי טאב · נוצר בבינה מלאכותית