פישינג: איך לא ליפול בפח – דף עבודה

מסלול רגיל

שם: _____ כיתה: _____ תאריך: _____

חלק א׳: קוראים את הטקסט

1. מה זה פישינג – ולמה זה קשור לכסף שלנו?

פישינג (Phishing, מהמילה האנגלית fishing – דיג) הוא תרגיל שבו נוכלים "זורקים פיתיון" ומחכים שמישהו ינשוך. הפיתיון הוא הודעה, מייל או שיחת טלפון שנראים כאילו הגיעו מגוף מוכר – בנק, חברת שליחויות, העירייה, חברה מהכיתה או אפילו בן משפחה. בעברית קוראים לזה גם דִּיוּג.

המטרה של הנוכלים כמעט תמיד היא כסף. הם לא צריכים לפרוץ לבנק – מספיק שאדם אחד ימסור להם את ה"מפתח": סיסמה, מספר כרטיס אשראי, מספר תעודת זהות או קוד חד־פעמי שנשלח אלינו בהודעה. עם הפרטים האלה אפשר לבצע קניות על חשבוננו, להיכנס לחשבון, להשתלט על אפליקציית ההודעות שלנו ולבקש כסף מהחברים שלנו בשמנו.

בחינוך פיננסי אנחנו לומדים לתכנן תקציב, לחסוך ולקנות בחוכמה. שמירה על הכסף והפרטים שלנו מפני הונאות היא חלק מאותה מיומנות: כסף שהרווחנו בעבודה, קיבלנו במתנה או חסכנו לאורך זמן יכול להיעלם בלחיצה אחת.

2. באילו צורות זה מגיע?

הודעת SMS מתחזה (סְמִישִׁינְג) – "החבילה שלכם מחכה, שלמו דמי משלוח", "יש לכם קנס שלא שולם", "החשבון שלכם נחסם".

מייל מתחזה – נראה רשמי, עם לוגו וצבעים של חברה מוכרת, ומבקש "לאמת פרטים" בקישור.

הודעה מ"חבר" או מ"בן משפחה" – "החלפתי מספר, תעבירו לי כסף דחוף". לפעמים זה חשבון של חבר אמיתי שנפרץ.

"זכיתם בפרס!" – הגרלה שלא השתתפתם בה, ורק צריך "לשלם דמי משלוח" או למלא פרטים.

אתר קניות מזויף ומבצע טוב מדי – מוצר יקר במחיר מגוחך, "נשארו רק 2 יחידות", ותשלום בהעברה לאדם פרטי.

שיחת טלפון מתחזה (וִוישִׁינְג) – "מדברים מהבנק, תקריאו לנו את הקוד שקיבלתם".

קוד QR מזויף – מדבקה שמודבקת מעל קוד אמיתי, למשל על מדחן חניה, ומובילה לאתר תשלום מתחזה.

3. סימני אזהרה: איך מזהים פישינג?

דחיפות ולחץ – "תוך שעה", "אחרת החשבון ייסגר", "רק היום". הנוכלים רוצים שנפעל מהר, בלי לחשוב.

שולח לא מוכר – מספר משונה, שם כללי כמו "שירות לקוחות", או מספר חדש שטוען שהוא מישהו שאנחנו מכירים.

כתובת קישור מוזרה – אותיות מוחלפות, סיומת לא מוכרת, כתובת ארוכה ומבולבלת.

שגיאות כתיב וניסוח מוזר – "לקוח יקר", משפטים מתורגמים, סימני קריאה רבים.

בקשה לקוד, לסיסמה או לפרטי כרטיס – גוף אמיתי לא יבקש מאיתנו קוד חד־פעמי או סיסמה.

"זכיתם!" – בלי שהשתתפנו בשום הגרלה.

תשלום בדרך משונה – כרטיסי מתנה, העברה מהירה לאדם פרטי, "דמי שחרור" קטנים.

"אל תספרו לאף אחד" – בקשה לשמור בסוד היא דגל אדום גדול.

4. חוקי הזהב – ומה עושים אם זה כבר קרה

חוקי הזהב: (1) קוד חד־פעמי לא מוסרים לאף אחד – אף פעם, גם לא ל"נציג הבנק". (2) לא לוחצים על קישור בהודעה – נכנסים בעצמנו לאפליקציה או לאתר הרשמי. (3) עוצרים ובודקים עם הורה או מבוגר שסומכים עליו; ל"חבר" שמבקש כסף מתקשרים למספר המוכר. (4) מפעילים אימות דו־שלבי בכל חשבון חשוב. (5) בוחרים סיסמה חזקה ושונה לכל חשבון – למשל משפט ארוך שקל לנו לזכור.

אם זה כבר קרה: לא מתביישים – זה קורה גם למבוגרים וגם לאנשים זהירים. (1) מספרים מיד להורה או למבוגר. (2) אם נמסרו פרטי כרטיס – מתקשרים מיד לבנק או לחברת האשראי כדי לחסום את הכרטיס. (3) מחליפים סיסמאות, ומתחילים בתיבת המייל. (4) מדווחים: מוקד 119 של מערך הסייבר הלאומי פועל בכל שעות היממה ומקבל דיווחים על פישינג והתחזות. אם נגנב כסף – מגישים גם תלונה במשטרה.

המחיר של הונאה הוא לא רק הכסף שנעלם: יש גם זמן, לחץ, חשבונות שצריך לשחזר ופרטים שכבר "יצאו" לעולם. צרכנים נבונים עוצרים לפני כל תשלום ושואלים: מי מבקש? למה עכשיו? האם המחיר הגיוני? איך אני יכולה או יכול לבדוק בעצמי?

חלק ב׳: שאלות על הטקסט

1. מה המטרה העיקרית של הנוכלים בפישינג?

א. להגיע לכסף או לפרטים האישיים שלנו

ב. לשלוח לנו פרסומות

ג. לבדוק אם הטלפון עובד

2. מה ההבדל בין סמישינג לווישינג?

א. סמישינג בהודעת SMS, ווישינג בשיחת טלפון

ב. סמישינג במייל, ווישינג באתר

ג. אין הבדל

3. "נציג הבנק" מבקש את הקוד שקיבלתם. מה נכון?

א. גוף אמיתי לא מבקש קוד חד־פעמי – מנתקים

ב. מוסרים, כי זה הבנק

ג. מוסרים רק חצי מהקוד

4. איזה מהבאים הוא סימן אזהרה?

א. "רק היום! אחרת החשבון ייסגר"

ב. הודעה בלי קישור שרק מזכירה תור

ג. הודעה מחברה מהכיתה ששואלת על שיעורי בית

5. הסבירו במילים שלכם: למה הנוכלים רוצים דווקא את הקוד החד־פעמי?

6. בחרו שני סימני אזהרה מהטקסט ותנו לכל אחד דוגמה משלכם.

7. מה "המחיר" של הונאה, מלבד הכסף שנעלם? כתבו שני דברים.

8. ראיתם מבצע: "נעלי ספורט ב־40 ₪ במקום 450 ₪". מה תבדקו לפני שתשלמו?

חלק ג׳: אמיתית או פישינג?

קראו כל הודעה. סמנו X בעמודה המתאימה.

#	ההודעה	אמיתית	פישינג
1	Parcel-IL: החבילה שלכם עוכבה. לשחרור יש לשלם 6.90 ₪ תוך 3 שעות: parcel-il-24.top/pay		
2	הבנק: קוד האימות שלכם: 482913. לעולם אל תמסרו את הקוד לאף אחד, גם לא לנציג הבנק.		
3	מספר לא שמור: 053-0000000: היי אמא, זו אני. הטלפון שלי נשבר וזה המספר החדש. תעבירי לי דחוף 1,800 ₪, אסביר אחר כך		
4	תמיכה <support@acount-verfy.net>: לקוח יקר, זיהינו פעילות חשודה. אם לא תאמת את פרטיך תוך שעה החשבון ייסגר לצמיתות. לאימות לחץ כאן.		
5	יעל מהכיתה: מישהו רשם מה צריך להביא מחר לטיול?		

6	WIN-PRIZE: ברכות!!! זכית בהגרלת החג: טלפון חדש מחכה לך. לקבלת הפרס שלם 9 ₪ דמי משלוח: prize-win-il.click		
7	שיחה נכנסת: מספר חסוי: "שלום, מדברים ממחלקת האבטחה של הבנק. יש חיוב חשוד בכרטיס. כדי לבטל אותו, תקריאו לי את הקוד שקיבלתם עכשיו בהודעה."		
8	העירייה: תזכורת: מחר, יום שלישי, יתקיים איסוף גזם בשכונה. אין צורך להשיב להודעה זו.		
9	חנות "סופר־דיל": סוף עונה! אוזניות אלחוטיות ב־39 ₪ במקום 899 ₪. נשארו 2 יחידות! תשלום בהעברה לחשבון פרטי בלבד.		
10	מדבקה על מדחן החניה: סרקו לתשלום מהיר ומוזל! (המדבקה מודבקת מעל הקוד המקורי)		
11	המורה לחינוך <mehanechet@school.example>: שלום לתלמידות ולתלמידים, דף העבודה לשיעור הבא נמצא במערכת בית הספר. נתראה ביום ראשון.		
12	קבוצה: "מתנות לכולם": רק היום! כרטיס מתנה של 500 ₪ לכל מי שממלא סקר ומעביר ל־10 חברים. מלאו פרטי אשראי "לאימות גיל".		

חלק ד׳: מצאו את סימני האזהרה

הקיפו בהודעה את החלקים החשודים, וכתבו מתחת למה הם חשודים.

מאת: Parcel-24 · לקוח יקר, החבילה שלך עוכבה במחסן. יש לשלם 6.90 ₪ דמי שחרור תוך 3 שעות אחרת היא תוחזר לשולח. לתשלום: parcel24-il.top/pay

---

מאת: service@my-bnk-update.net · נושא: דחוף!!! החשבון שלך ייחסם · שלום לקוח נכבד, זיהינו כניסה חשודה לחשבון. כדי לשמור על הכסף שלך, הקלד שם משתמש, סיסמה ומספר כרטיס בקישור המצורף. החשבון ייסגר לצמיתות אם לא תפעל עכשיו. בברכה, צוות האבטחה

מספר לא שמור: 053-0000000 · היי, זאת אני, נועה! החלפתי מספר. אני בבעיה קטנה. צריכה שתעבירי לי 400 ₪ עכשיו לחשבון של חבר שלי. אל תספרי לאף אחד, אני מתביישת. אחזיר לך מחר.

חלק ה׳: מה עושים עכשיו?

1. קיבלתם הודעה שחבילה מחכה ויש לשלם 5 ₪. לא הזמנתם כלום.

א. מוחקים את ההודעה ולא לוחצים על הקישור

ב. לוחצים רק כדי לבדוק מה יש שם

ג. עונים לשולח: "מי אתם?"

2. מישהו מתקשר "מהבנק" ומבקש את הקוד שקיבלתם עכשיו.

א. מנתקים, מספרים להורה, ואם צריך מתקשרים לבנק במספר הרשמי

ב. מקריאים את הקוד – הרי זה הבנק

ג. מקריאים רק חלק מהקוד

3. "חבר" כותב ממספר חדש ומבקש שתעבירו לו 300 ₪ דחוף.

א. מתקשרים לחבר במספר המוכר ושואלים אותו ישירות

ב. מעבירים מהר, הוא הרי חבר

ג. שולחים לו את פרטי הכרטיס של ההורים

4. כבר לחצתם על קישור והקלדתם את הסיסמה שלכם.

א. מספרים מיד למבוגר, מחליפים את הסיסמה ומפעילים אימות דו־שלבי

ב. מחכים לראות אם יקרה משהו

ג. מוחקים את ההודעה ושותקים מבושה

5. הקלדתם את פרטי הכרטיס של ההורים באתר שהתברר כמזויף.

א. מספרים להורים מיד, והם מתקשרים לבנק או לחברת האשראי לחסום את הכרטיס

ב. מקווים שזה יסתדר לבד

ג. מנסים לקנות שוב באותו אתר

6. מצאתם אתר שמוכר נעלי ספורט ב־80% הנחה.

א. בודקים את כתובת האתר, ביקורות ושיטת תשלום מאובטחת, ומתייעצים עם מבוגר

ב. קונים מהר לפני שייגמר

ג. משלמים בהעברה לחשבון פרטי כמו שביקשו

חלק ו׳: כרטיס יציאה

דבר אחד חדש שלמדתי היום על פישינג:

סימן אזהרה שאזהה מעכשיו:

למי אפנה אם אקבל הודעה חשודה: