# הגברת מודעות פיננסית

# שבוע המודעות להונאות דיגיטליות

---

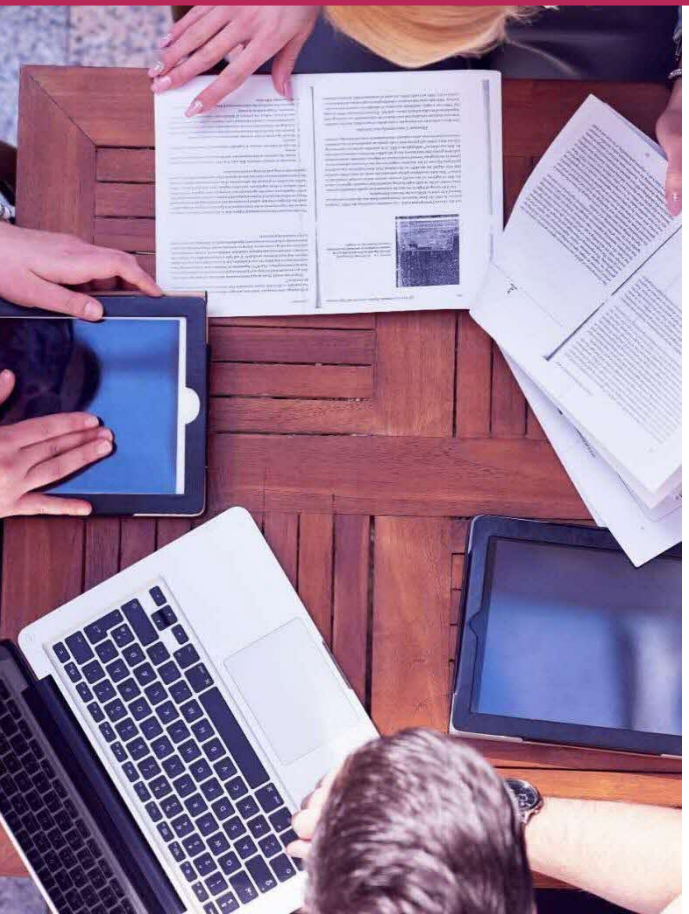
**הפיקוח על הבנקים בבנק ישראל באמצעות איגוד הבנקים, המערכת הבנקאית וחברות כרטיסי אשראי**

# הונאות דיגיטליות

איך נזהה אותן ונזהר מפניהן

הגברת מודעות פיננסית

# נושאי המפגש



- ✓ מהי הונאה דיגיטלית?
- ✓ סוגי הונאות
- ✓ איך נזהה?
- ✓ איך נזהר?
- ✓ העוקץ הרוסי

הגברת מודעות פיננסית

# מהי הונאה דיגיטלית?

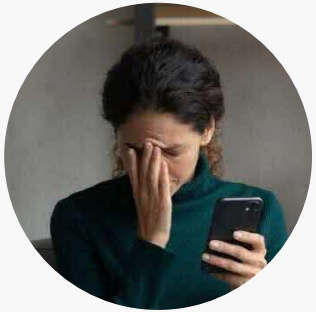
- הונאה דיגיטלית היא סוג של פשע סייבר – בה התוקפים מרמים את המשתמשים בדרכים שונות וכך מצליחים לגנוב פרטים אישיים שבאמצעותם יוכלו להתחזות אליהם ולעשות פעולות בשמם.
- הנוכלים פונים באמצעות הודעת סמס לטלפון הנייד או בשיחת טלפון, בכדי לגנוב פרטי הזדהות או כרטיס אשראי לצורך העברת כספים, כניסה לחשבון הבנק או לצורך ביצוע פעולות רכישה.

# למה זה קורה?

מהן הסיבות לביצוע ההונאות?

השגת מידע

רווח כספי



שיבוש, מעקב
או השבתה

השתלטות על פרופיל
ברשת חברתית

הגברת מודעות פיננסית

# איך זה נראה?



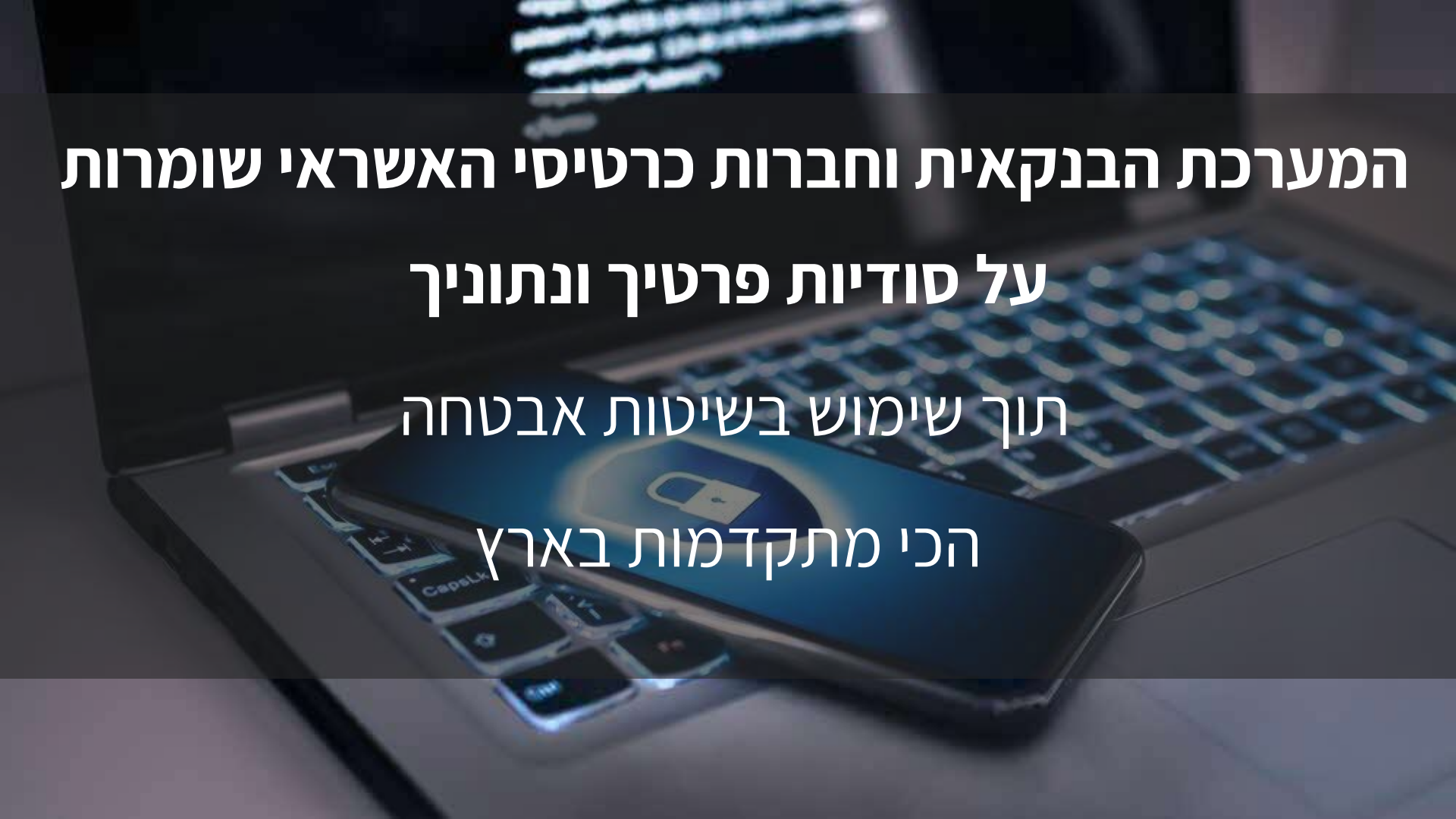





הגברת מודעות פיננסית

# האם מישהו קיבל הודעה כזו?

הגברת מודעות פיננסית



# המערכת הבנקאית וחברות כרטיסי האשראי שומרות על סודיות פרטיך ונתוניך

תוך שימוש בשיטות אבטחה

הכי מתקדמות בארץ

**הבנקים וחברות כרטיסי האשראי לעולם לא יבקשו שנזין במייל פרטי חשבון או כרטיס אשראי**

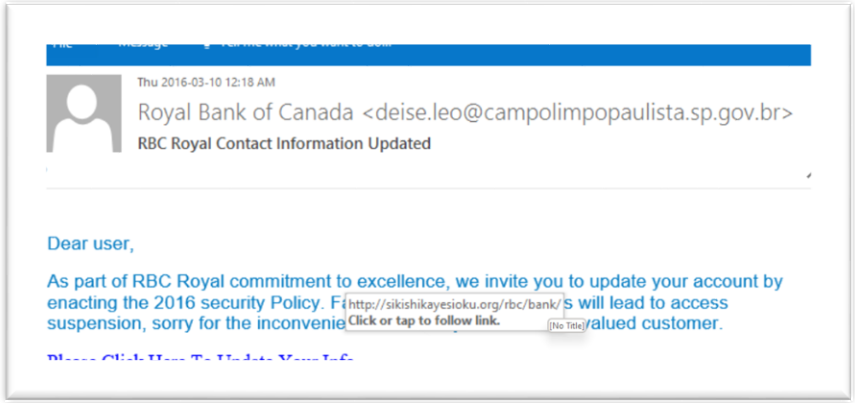
אך חשוב שנפעל בזהירות ונגלוש בטוח

# שיטות הונאה

הגברת מודעות פיננסית

# פישינג- באמצעות דוא"ל

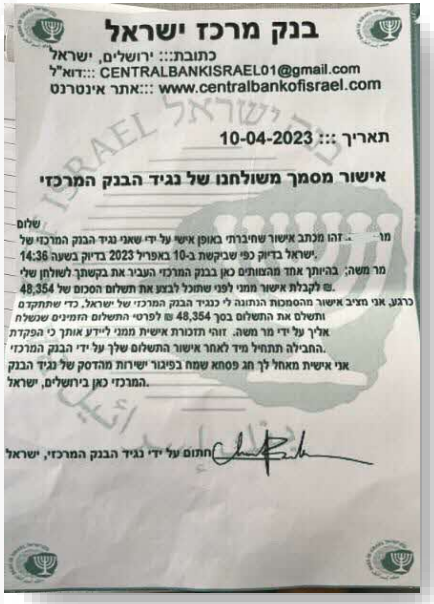
- פישינג- התוקף פונה לתפוצה רחבה של אנשים ומנסה "להעלות ברשתו" מידע אישי רגיש או פיננסי של המשתמש
- השיטה הנפוצה ביותר היא התחזות לאתר מוכר או מוסד פיננסי
- המטרה – לגרום לקורבן למלא טופס מזויף או לגשת לאתר האינטרנט ולהזין את פרטי הכניסה/פרטים אישיים
- האתרים יכולים להיות דומים לאתר המקורי גם ויזואלית וגם בכתובת ה-URL (כתובת של דף האינטרנט באתר)




הגברת מודעות פיננסית

# דוגמה להונאת פישינג

שליחת מכתבים מטעם בנק ישראל בצירוף מסמכים מזויפים



בנק מרכז ישראל

כתובת::: ירושלים, ישראל

דוא"ל::: CENTRALBANKISRAEL01@gmail.com

אתר אינטרנט::: www.centralbankofisrael.com

תאריך ::: 10-04-2023

אישור מסמך משולחנו של נגיד הבנק המרכזי

שלום

מר [illegible] זהו מכתב אישור שחיברתי באופן אישי על ידי שאני נגיד הבנק המרכזי של ישראל בדיוק כפי שביקשת ב-10 באפריל 2023 בדיוק בשעה 14:36.

מר משה, בהיותך אחד מהמוותים כאן בבנק המרכזי העביר את בקשתך לשולחן שלי לקבלת אישור ממני לפני שתוכל לבצע את תשלום הסכום של 48,354 ₪.

כרגע, אני מציב אישור מהסמכות הנתונה לי כנגיד הבנק המרכזי של ישראל, כדי שתתקדם ותשלם את התשלום בסך 48,354 ₪ לפרטי התשלום המזויפים שנשלח אליך על ידי מר משה. זוהי תזכורת אישית ממני ליידע אותך כי הפקדת התביעה תתחיל מיד לאחר אישור התשלום שלך על ידי הבנק המרכזי.

אני אישית מאחל לך חג פסחא שמח בפיקוח ישירות מהדסק של נגיד הבנק המרכזי כאן בירושלים, ישראל.

חתום על ידי נגיד הבנק המרכזי, ישראל

הבנק המרכזי של ישראל

כתובת::: ירושלים, ישראל

דוא"ל::: CENTRALBANKISRAEL01@gmail.com.

אתר אינטרנט::: www.centralbankofisrael.com

קבלה בנקאית מקורית

תאריך ::: 04-08-2023

שקלים 40,295

(לאישור הפקדת חבילה לחשבונות הבנק של

| | |
|---|---|
| סכום כולל | 120,885 שקלים |
| סכום שהתקבל | 40,295 שקלים |
| יתרה לתשלום | 80,590 שקלים |

תשלום שהת

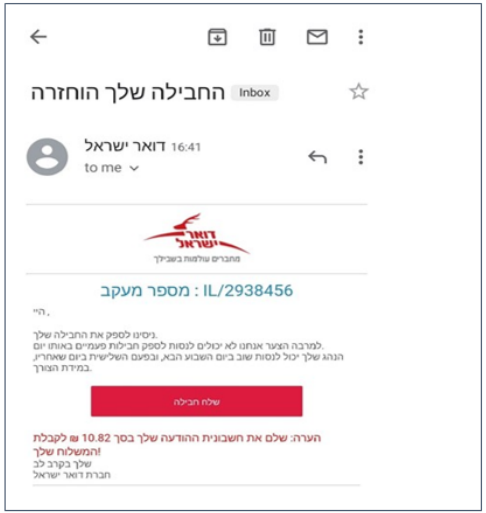
הגברת מודעות פיננסית

# דוגמה להונאת פישינג

הונאה באמצעות התחזות לדואר ישראל
הלקוח מנסה לשלם סכום מסוים לדואר ישראל.
בפועל התשלום המתבצע הוא בסכום גבוה יותר ולבית עסק אחר

"להעברת תשלום בסך ILS 1075.00 באופן סופי מכרטיס 6043 לMISRADHTACHBU יש להקליד את הקוד באתר.
*חשוב לדעת* הקוד הוא רק שלך ואסור למסור אותו לאף אדם, לא מבית העסק ולא מחברת האשראי. אם לא ביצעת עסקה, יש לדווח מיד ל- 03-4564564

קוד האימות הוא ******..."




הגברת מודעות פיננסית

# דוגמה להונאת פישינג

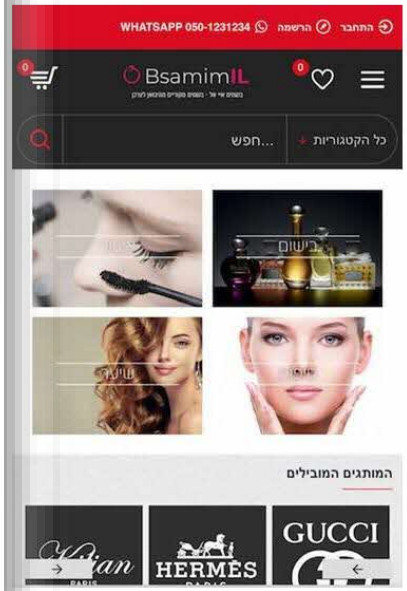
הונאות מעולם כרטיסי אשראי

(!) בעסקאות מאובטחות הדורשות הזנת קוד בטחון חד פעמי חשוב לשים לב לסכום המצוין בהודעה, למטבע העסקה ולשם בית העסק:

להעברת תשלום בסך 135.00 ILS באופן סופי מכרטיס 8717 לNEXT יש להקליד את הקוד באתר.
**חשוב לדעת** הקוד הוא רק שלך ואסור למסור אותו לאף אדם, לא מבית העסק ולא מחברת האשראי.
אם לא ביצעת עסקה, יש לדווח מיד ל- 03-6177750 קוד האימות הוא 953003

תרגום לרוסית:
В данный момент, по вашей кредитной карте которая заканчивается на 8717 проходит оплата в интернете, на сайте NEXT на сумму 135.00ILS
Код, полученный на ваш телефон предназначен для завершения платежа - не передавайте его посторонним лицам, включая представителей банка кредитной и компании!
Если вы не совершали эту покупку, срочно позвоните по телефону 03-6177750.
Код подтверждения 953003
@max.co.il #953003

14:26


הודעה
היום 17:58

שלום,
יש חבילה שהגיעה לארץ וצריך לשלם 14.35₪
עבור שחרור ממכס
מספר מעקב :
CN801486IL
לתשלום דרך הקישור הזה:
https://bungamati.com/14..35/

הגברת מודעות פיננסית

# פישינג- באמצעות מסרון או הודעת WhatsApp עם קישור

- הודעה נשלחת לקורבן באמצעות מסרון או ווטס אפ ומכילה קישור הקוראת לפעולה לגיטימית
- לעיתים עצם הלחיצה על הקישור מאפשרת להאקר גישה למכשיר
- דוגמאות לכך: רישום לאירוע, ביצוע תשלום, קבלת משלוח, מבצעים אטרקטיביים, הורדת אפליקציה וכדומה


הגברת מודעות פיננסית

# וישיניג - הונאה המתבצעת באמצעות שיחות טלפון

- מתקשרים לקורבן ומתחזים לגורם לגיטימי בעיקר בשני נושאים:
  - התחזות לשוטר, גורם בטחון של הבנק או של חב' כרטיסי אשראי
  - פניה בנושא צרכני/השקעה
- מבקשים פרטי חשבון תחת סיפור כיסוי – התראה על החשבון, הצעה שיווקית וכדומה
- בעזרת מספר הטלפון/ת.ז או סיסמא של הקורבן, לנוכל יש קצה חוט למבצע עוקץ

# וישיניג- באמצעות שיחות טלפון מזויפות

הגברת מודעות פיננסית

# שיחות טלפון מזויפות לכאורה מהבנק

## איך זה נשמע?

"שלום מדברים מהבנק אנחנו מעדכנים לכל הלקוחות שלנו את האפליקציה כדי לקבל התראות והטבות".

שיתקשרו אלי מהסניף

לא עושים את זה דרך הסניף, שלחתי לך כרגע הודעה

אוקי מה אתה צריך ממני?

רק לקבל את הקוד ששלחתי לך בסמס

הגברת מודעות פיננסית

# איך זה נשמע?

"שלום מדברים מחברת כרטיסי האשראי אנחנו מזהים שיש פעילות חריגה בכרטיס האשראי שלך"

מה באמת, מה אתם רואים?

"יש עסקאות בסכומים חריגים מעבר לעסקאות הרגילות בכרטיס 4455"

אוקי מה אתה צריך ממני?

"כדי לעצור את החיובים ולוודא שזה אתה אני צריך את מס' כ. האשראי, מס' ת.ז. ובהמשך את הקוד ששלחתי אליך

הגברת מודעות פיננסית

# שיחות טלפון מזויפות לכאורה מחברת כרטיסי אשראי

# מה אתם הייתם עושים?

**במידה וקיבלתם שיחת טלפון כזו איך הייתם מגיבים?**

1. מספקים להם מיד את המידע שביקשו.
2. שואלים למה הם צריכים את המידע ומספקים רק את מה שהם צריכים.
3. מסרבים למסור פרטים אישיים כלשהם ולנתק.
4. אומרים להם שאין לנו פרטים אישיים למסור להם ומדווחים למשטרה.
5. מתקשרים באופן יזום לבנק /חכ"א.

הגברת מודעות פיננסית

**הבנקים וחברות כרטיסי האשראי לעולם לא יפנו אליכם לקבלת פרטים חסויים,**

אלא רק אתם אליהם!

# איך נזהה?

# סימנים מחשידים

שגיאות כתיב

פניה דחופה

פניה שאינה אישית

שפה זרה

שליחת קישור לחשבונך האישי

התחזות לנציג משטרה

הגברת מודעות פיננסית

# המלצות לפעולה

- לבקש מהנציגים לדבר בעברית
- לשאול לשם ותפקיד בבנק או בחברת כרטיסי אשראי
- להתקשר באופן יזום לבנק או לחברת כרטיסי האשראי
- לא לבצע בקשות חשודות כמו משיכת כספים
- לא למסור פרטים כשאינך הגורם היוזם את השיחה
- לרשום את המספר ממנו התקשרו
- לדווח לבנק או לחברת כרטיסי האשראי ולהגיש תלונה במשטרה

# בואו נבדוק אם הבנו...

## האם ההצעה הזו תקינה או לא?

קיבלתם שיחת טלפון מגורם שמזדהה כנציג הבנק שמספר לכם שהתקבלו חיובים חריגים בכרטיס האשראי שלכם ועל מנת לבדוק ולטפל בנושא כל מה שאתם מתבקשים זה לתת לו את פרטי הכרטיס

# בואו נבדוק אם הבנו...

## האם ההצעה הזו תקינה או לא?

שלום, אנו חברת ביטוח ואנו מציעים כחלק משירותינו לבדוק את הביטוחים הקיימים לכם, כדי למנוע כפילויות. נשמח לקבל את תעודת הזהות שלכם, ופרטי ההזדהות שלכם לאתר "הר הכסף" כדי לבדוק את הביטוחים שלכם.

# בואו נבדוק אם הבנו...

## האם ההצעה הזו תקינה או לא?

קיבלתם הודעת SMS מהבנק שלכם שמתריעה כי יש כמה בעיות בחשבון הבנק ואתם מתבקשים להקליק על הקישור ולעדכן את פרטי החשבון

?


הגברת מודעות פיננסית

# איך ניזהר?


הגברת מודעות פיננסית

# אילו פעולות ניתן לעשות כדי להיות בטוחים יותר

סיסמה חזקה
וייחודית / זיהוי
ביומטרי

הימנעות מלחיצה
על קישורים

היו קנאים
לפרטיותכם

הורדת אפליקציות
מחנויות רשמיות

רשת מאובטחת

הגברת מודעות פיננסית

# סיסמה חזקה וייחודית

## עשו

- שילוב מספרים ואותיות שקל לנו לזכור אבל אין להם משמעות לאחרים
- צירוף סימנים ייחודיים !@#$
- זיהוי ביומטרי (טביעת אצבע/זיהוי פנים)

## אל תעשו

- ציון תאריך לידה בלבד
- מספר זהות בלבד
- רצף פשוט של אותיות/מספרים

## טיפים להגנה על הסיסמה

- אין לשתף את הסיסמה עם אף אחד
- אין לשמור את הסיסמה בשום מקום
- אף אתר לעולם לא יבקש מכם סיסמא בטלפון או בסניף – היא שלכם בלבד

## דוגמאות לסיסמה חזקה

- #@Haifa1957
- Zehava90210
- Batman156 !

הגברת מודעות פיננסית

# הימנעות מלחיצה על קישורים

לא פותחים קישורים חשודים שהגיעו ב-SMS או במיילים מגורמים לא מוכרים

מאמצים גישה כללית של חשדנות וזהירות

אם יש בעיה או הטבה בחשבון, תקבלו על כך הודעה עם כניסתכם לחשבונכם באפליקציה/באתר


הגברת מודעות פיננסית

# הורדת אפליקציות מחנויות רשמיות

**הורידו את האפליקציה הרשמית של הבנק/חברת כרטיסי האשראי מחנות האפליקציות ולא מקישור**

סמל החנות במכשיר
**מסוג אייפון**

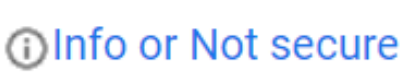
סמל החנות במכשיר
**מסוג אנדרואיד**

הגברת מודעות פיננסית

# גלישה ברשת מאובטחת

## פעולות רגישות לא עושים ברשת WI-FI ציבורית


## דוגמאות לאתרים לא מאובטחים





הגברת מודעות פיננסית

# גלישה ברשת מאובטחת

## דוגמאות לצעדים שנוכל לבצע שיגנו עלינו

- במידה והמחירים באתר זולים באופן מוגזם או שמצוין בו שהמחירים במיוחד לישראלים, זה צריך להעלות חשד.
- כדאי לבדוק המלצות ודירוגים של אתרים / חנויות לפני שמקלידים את פרטי התשלום.
- עדיף לבצע רכישה בשימוש כרטיס אשראי נטען שהוא מוגבל בסכום או דרך שירותי תשלום שמאפשרים לקבל החזר כספי.
- אשרו קבלת התראות על עסקאות בסכומים גבוהים והוצאות בחו"ל/באינטרנט באפליקציית חברת כרטיסי האשראי.

הגברת מודעות פיננסית

# היו קנאים לפרטיותכם

- היו ערניים למה שאתם מפרסמים ברשת ומומלץ גם לשמור על החשבונות ברשתות החברתיות שלכם נעולים
- אל תספקו מידע - שימו לב כי בנקים או חברות כרטיסי האשראי לא יבקשו מכם פרטים אישיים כמו סיסמה או פרטי כרטיס אשראי
- אל תמסרו פרטים בכתב/ בטלפון/ כאשר לא אתם יזמתם את השיחה.

הגברת מודעות פיננסית

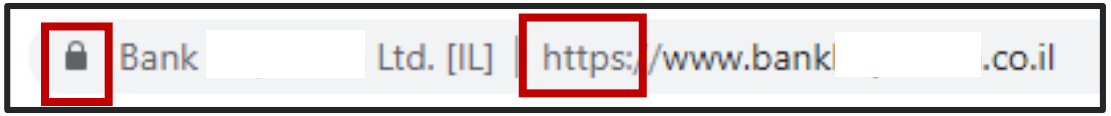
# המלצות לאבטחת חשבון הבנק/ האזור האישי בחברת כרטיסי אשראי

- מסרו פרטי זיהוי אך ורק לאחר ביצוע שיחה חוזרת למוקד הבנק/לחברת כרטיסי האשראי למס' הטלפון אותו איתרתם בעצמכם באתר הרשמי
- לא למסור פרטי חשבון / כרטיס אשראי – במיוחד כאשר לא יזמתם את השיחה
- טעיתם ומסרתם? – פנו באופן מידי לבנק/לחברת כרטיסי האשראי ודווחו על כך
- עקבו אחר הפעילות הבנקאית/פירוט חיובי כרטיסי האשראי דרך האתר או אפליקציה באופן שוטף, שימו לב לתנועות חשודות או אי התאמות
- אשרו קבלת התראות על עסקאות בסכומים גבוהים ורכישות בחו"ל/באינטרנט, באפליקציית חברת כרטיסי האשראי
- אם יש ספק – אין ספק ומוטב לא להיענות להודעה, מאשר להיכנס לקישור לא מאובטח

הגברת מודעות פיננסית

# איך להתחבר לחשבונכם בדיגיטל?

1. חיפוש בנק או חברת כרטיסי אשראי X בגוגל או הקלדת כתובת האתר בשורת החיפוש.
2. וודאו שמדובר באתר מאובטח ואמין שמאוית נכון.




3. שימוש באפליקציית הבנק/ חברת כרטיסי האשראי המותקנת במכשיר.

**אל תתחברו לחשבון מתוך מסרון או דוא"ל שאתם מקבלים**

הגברת מודעות פיננסית

# העוקץ הרוסי

הונאות פיננסיות
זה לא צחוק!

הגברת מודעות פיננסית

# מה זה העוקץ הרוסי?

- שיטת ההונאה שזכתה לכינוי "העוקץ הרוסי" הפילה בפח כבר עשרות מבוגרים - **רובם יוצאי חבר העמים.**
- באמצעות שימוש באפליקציות מיוחדות המאפשרות **להתחזות בשיחת טלפון למשטרה או לבנק.**


N12

כל החדשות | פוליטי | ביטחוני | פלילי | בעולם | כלכלה | DATA12 | ספורט | המגזין | תרבות | פנים | חינוך | תוכניות

פלילי

**מזדהים כשוטרים – ועוקצים קשישים: "הכסף הזה ללוויה שלי"; "יקברו אותך גם כבה"**

עשרות מבוגרים - רובם יוצאי חבר העמים •
את הקוד לאפליקציה, הייתי בטוחה שאני
מתקשר? המדריך המלא

00:56


# העוקץ הרוסי: תושב העיר חשוד בהונאת מיליונים

על פי החשד, כ-20 קורבנות, מרביתם דוברי רוסית, העבירו לחשוד כספים בסך כ-4.5 מיליון שקל, לאחר שהתחזה לעובד בנק או חברת אשראי. בימים הקרובים יוגש נגד החשוד כתב אישום

אלון חכמון 09:39 14/12/2022 2 דק' קריאה

הגברת מודעות פיננסית

# כיצד מתבצע העוקץ?

- הנוכלים משתמשים בתעודות רשמיות מזויפות – כמו תעודת שוטר/מסמכים מגופים ממשלתיים/ציבוריים, למשל בנק ישראל
- מבצעים שימוש באמצעי תשלום שלא בהסכמת הקורבן וקבלת דבר במרמה של האוכלוסיות המבוגרות




# איך השיטה עובדת?

## שלב ראשון

שיחה לקורבן - התחזות לנציג מטעם בנק/חברת אשראי

שלום, תקוה, מדבר תת ניצב מייקל ממשטרת ישראל . צר לי לבשר לך שכספך בבנק נמצא בסכנה.

מה זאת אומרת בסכנה? מה זה אומר?

נפלת קורבן להונאה כספית, כדאי שתיגשי לבנק לבקש סיסמה לבנקאות בתקשורת.

אף אחד לא דיבר איתי על זה מהבנק, אני רוצה לבדוק את זה. זה נשמע לי חשוד מידי.

אני מבין, זה מאוד מפחיד. אבל אנחנו כאן כדי לשמור עליך ועל הכסף שלך. בכל מקרה, בשלב הראשון אני מציע לא לשתף את הבנק כי אנו חוששים שבבנק יש גורם שמסייע למקרה הונאה זה.

הגברת מודעות פיננסית

# איך השיטה עובדת?

**שלב שני**
בקשה להעברת פרטים

לאחר השיחה הראשונה, מתחזה נוסף מהבנק או חברת כרטיסי האשראי יוצר קשר עם הקורבן ומבקש פרטי זיהוי כולל גישה לחשבון הבנק במטרה לבלום את ניסיון הפריצה

הקורבן מרגיש מגויס למניעת הונאה ותפיסת החשודים

הגברת מודעות פיננסית

# איך השיטה עובדת?

**שלב שלישי**
העברת כספים

הקורבן מתבקש למשוך מזומנים ולהעבירם לידי שליח או להפקיד בחשבונות

צ'יינג'ים הפרוסים במקומות שונים בארץ

במקרים מסוימים הנוכל משתלט על החשבון –
ומבצע העברת כספים לחו"ל, הקמת הלוואות וכדומה

הגברת מודעות פיננסית

# איך נזהה ומה נעשה?

| זיהוי | פעולה |
| --- | --- |
| הנוכל מבקש את פרטי ההזדהות של הלקוח לחשבון הבנק | נציגי הבנק/חברת כרטיסי אשראי לעולם לא יבקשו מלקוחות פרטי הזדהות וכניסה לחשבון הפרטי. לכן לעולם לא למסור שום פרט בשיחה נכנסת או הודעה |
| הנוכל טוען שאתם חייבים כספים | בדקו מסמכים שמעידים על חוב |
| הנוכל מבקש לשמור את המידע ולא לספר לשום גורם מקצועי או במשפחה | בכל מצב, התייעצו עם בני משפחה, עובדי בנק/חברת כרטיסי אשראי שהנכם מכירים, שוטרים קהילתיים וכדומה |

**מקדימים תרופה למכה – מעלים מודעות להונאות קיימות במעגלים הקרובים, במיוחד בקרב בני משפחה וחברים**

הגברת מודעות פיננסית

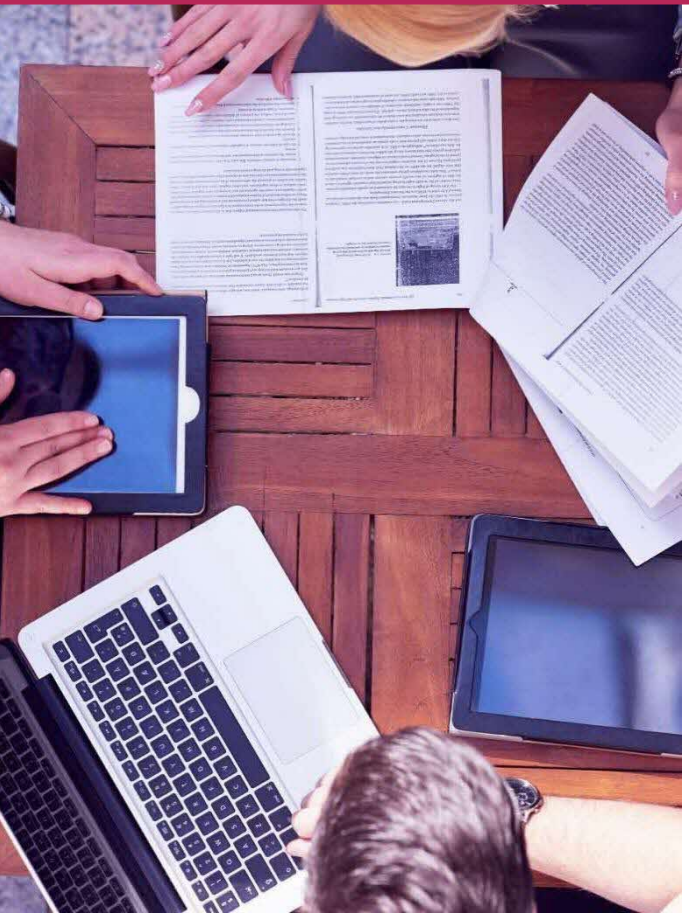
# מה אתם הייתם עושים?

## כיצד הייתם פועלים כדי לעזור לבן משפחה לא ליפול להונאה?


1. מעלים את המודעות - מספרים על מקרי הונאה שקרו, ושולחים כתבות וסרטונים על מקרים כאלו אחת לכמה זמן
2. לוקחים את המכשיר הנייד וחוסמים אותו לשיחות, הודעות ורשתות חברתיות
3. שותלים האזנה בטלפון
4. בודקים את הטלפון למספרים חשודים ואנשי קשר לא רלוונטיים
5. בודקים את חשבונות הבנק יחד, מגבילים רכישות און ליין, ושואלים האם קיבלו שיחות עם הצעות לעסקאות?

הגברת מודעות פיננסית

# סיכום



- ✓ הונאות דיגיטליות הן בין המתקפות הנפוצות והיעילות בשימוש תוקפים בעולם הסייבר, ואף התעצמו בשנים האחרונות.
- ✓ פישינג עשוי להגיע כפנייה במייל, מסרון או שיחת טלפון ולייצר לחץ למסירת פרטים תוך התחזות לגורם לגיטימי.
- ✓ הכלי החזק ביותר שעומד לרשות הנוכלים הוא חוסר ידע של הקורבנות, לכן מודעות לסכנה תאפשר לכם להימנע ממנה בקלות יחסית.
- ✓ היעזרו בטיפים ובדרכי הזיהוי שלמדנו ושמרו על ערנות כדי להיות מוגנים כמה שיותר.
- ✓ **וזכרו! הבנקים וחברות כרטיסי האשראי לעולם לא יתקשרו אליכם ויבקשו מכם פרטים אישיים, פרטי חשבון או כרטיס.**

הגברת מודעות פיננסית

# שאלות?

הגברת מודעות פיננסית

# תודה על ההקשבה

הגברת מודעות פיננסית