כללים לגלישה בטוחה ומניעת הונאה

חברת בנק הדואר בע"מ ("**בנק הדואר**" או "**הבנק**") משקיעה מאמצים רבים ומשתמשת בטכנולוגיות מתקדמות של אבטחת מידע, כדי לאפשר לך גלישה מאובטחת ובטוחה. בעת שימוש בשירות "בנקאות ביתית" בקווי תקשורת ("**השירות**"), באמצעות אתר האינטרנט של הבנק ("**האתר**") ו/או דרך מכשיר הקצה שלך באמצעות האפליקציות השונות המוצעות על ידי הבנק ("**האפליקציה**"), מומלץ לנהוג אחר הכללים המפורטים להלן.

1. כללים לגלישה בטוחה

1.1. מומלץ להתחבר לשירות דרך האתר ו/או האפליקציה אך ורק מתוך רשת פרטית מאובטחת, ולא מנקודות גישה ציבוריות (בתי קפה, מסעדות וכד'). בשימוש בטלפון חכם, מחשב שולחני או נייד מומלץ להימנע משימוש במכשירים ציבוריים או במכשירים שרמת האבטחה בהם אינה ידועה. למשתמשים ברשת אלחוטית ביתית - מומלץ לאבטח את התקשורת האלחוטית באמצעות פרוטוקול הצפנה אלחוטי.

1.2. רצוי לוודא את זהותו של אתר הבנק בעת הכניסה אליו.
כתובת אתר בנק הדואר הינה: https://www.bankhadoar.co.il.
היו עירניים לסימנים מחשידים לכך שהאתר בו הנכם גולשים ו/או האפליקציה בה אתם עושים שימוש אינם אלו של הבנק.

1.3. מומלץ לסגור דפדפנים אחרים בעת הגלישה באתר ו/או באפליקציה.

1.4. חשוב להקפיד על ניתוק מהשירות, בסיום השימוש, על ידי לחיצה על כפתור "יציאה" הנמצא בחלקו העליון של הדף. אין להשאיר מחשב או כל מכשיר קצה אחר מחובר לאתר ללא השגחה. אם הנך עושה שימוש בשירות באמצעות אפליקציה, נא וודא סגירה מסודרת שלה בעת סיום השימוש.

1.5. רצוי להקפיד על התקנה ושימוש נאות בערכת הגנה של חברה מוכרת לאבטחת מחשבך האישי. מומלץ לוודא כי מערכת ההפעלה, מערכות ההגנה (פיירוול, אנטי וירוס) והדפדפן כוללים עדכוני אבטחת מידע אחרונים.

1.6. אם מותקנות במחשבך תוכנות שיתוף קבצים מסוגים שונים, עליך לוודא כי נתונים אישיים אינם נשמרים או משותפים במחשבך.

1.7. מומלץ להגדיר מחיקת קבצים זמניים באופן אוטומטי בסגירת הדפדפן.

1.8. הורידו את האפליקציה אך ורק מחנויות מורשות (למשל Apple Store או Google Play).

2. הונאות באינטרנט

2.1. אתר הבנק ו/או האפליקציה עשויים להיות יעד לניסיונות הונאת אינטרנט (Phishing) של גורמים עוינים, המנסים בכל עת לאסוף נתונים ופרטים חסויים של לקוחות על מנת לקבל גישה אל חשבונותיהם. דוגמא לפרטי זהות רגישים: מספר כרטיס חיוב, מספר תעודת זהות, סיסמת גישה לחשבון הבנק או נתונים אישיים אחרים. אחת השיטות הידועות הינה שליחת הודעת דואר אלקטרוני מתחזה הנשלחת כביכול מבנק הדואר, המכילות קישור לאתרים מתחזים ו/או המבקשת מהלקוח להשלים פרטים מזהים לגבי חשבון הבנק שלו. איום זה מחייב נקיטת אמצעי זהירות, הן על ידי הבנק והן על ידי לקוחותיו.

2.2. **לתשומת לבך: בנק הדואר אינו מבקש מלקוחותיו נתונים אישיים אודות חשבונות הבנק, או סיסמאות גישה למערכות הבנק**. אם התקבלה הודעת דואר שנשלחה כביכול מבנק הדואר, המבקשת ממך למסור פרטי חשבון או פרטי הזדהות לשירות, אנו מאוד מבקשים לדווח על כך למוקד התמיכה של בנק הדואר בטלפון: 02-5005303

2.3. יש למחוק מיד כל הודעת דוא"ל הנראית חשודה, מבלי לפתוח אותה.

2.4. סימנים להונאה בדואר אלקטרוני יכולים להיות, בין היתר, כל אחד מאלה: הודעות דואר אלקטרוני המבקשות במפורש שליחת פרטי הזדהות, הודעות "דחופות" המודיעות לך שחשבונך ייסגר אם לא תעדכן מיידית את פרטי הזיהוי שלך, הודעות הכתובות בשפה עילגת, הודעות שאינן ממוענות לאדם מסוים, הודעות שאינן חתומות דיגיטלית המכילות לינק לכניסה לאתר.

2.5. ככל והעברת פרטים אישיים (שם משתמש, סיסמא, מספר חשבון, מספר כרטיס חיוב, מספר תעודת זהות וכו') לאתר המתחזה לאתר בנק הדואר ו/או לכל צד שלישי שאינו מורשה יש לדווח על כך מיידית לבנק. ככל וביכולתך לשנות את סיסמתך, נא עשה זאת. אם העברת לאתר מתחזה את פרטי כרטיס החיוב שלך, עליך לדווח על כך מיידית לחברת כרטיסי החיוב.

2.6. בכל מקרה של חשש לפריצה ו/או הונאה באינטרנט, הבנק יהיה רשאי, בין אם על פי הודעתך ובין אם ביוזמת הבנק, לחסום את חשבונך האישי, לאתחלו מחדש על ידי הנפקה מחדש של קוד משתמש ו/או סיסמת גישה או להגבילו בתנאים (למשל, הגבלה לצפייה בלבד), על פי שיקול דעתו הבלעדי של הבנק. חשבון שנחסם ביוזמת הבנק ישוחרר רק ע"י הבנק.

3. <u>שימוש נכון בסיסמא</u>

כיצד יש לנהוג עם קוד המשתמש והסיסמא לשירות שקיבלת מבנק הדואר?

3.1. עליך להיכנס לשירות עם קוד המשתמש והסיסמא הראשונית תוך 30 יום מקבלתם ולהחליף את הסיסמא לסיסמא אישית. אם לא תתבצע כניסה לשירות בתוך 30 יום מהגדרת הסיסמא האישית, הסיסמא תיחסם ותיאלץ לקבל סיסמא חדשה ביחידת הדואר בו נרשמת לשירות. **זכור: קוד וסיסמת המשתמש הינם אישיים ואין להעבירם**.

3.2. מבלי לגרוע מהאמור לעיל, יש להחליף את הסיסמא האישית כל תקופה בת 180 יום ממועד החלפת הסיסמא הקודמת. יחד עם זאת, אנו ממליצים להחליף את הסיסמא האישית בתדירות גבוהה יותר. אי החלפת סיסמא בתום תקופה בת 180 יום תמנע גישה לחשבונך באתר ובכל הערוצים האחרים המחייבים הזדהות באמצעות אותם פרטי הזיהוי הדרושים לצורך גישה לחשבונך באתר. חסימת גישה לאתר תתבצע אוטומטית אם לא נרשמה כניסה לחשבונך באתר במשך 6 חודשים רצופים, והתרת החסימה תחייב תחילה הנפקת סיסמא ראשונית ביחידת הדואר בו נרשמת לשירות, או איפוס סיסמא והגבלת רמת השירות לצפייה בלבד.

3.3. מומלץ לבחור סיסמא איכותית שאינה קלה לניחוש. הרכב הסיסמא יכלול מינימום 8 תווים, המכילים לפחות 3 אותיות בלועזית מהן אחת גדולה ו-2 ספרות. מומלץ שהסיסמא תכיל גם סימנים מיוחדים, מבין הסימנים המופיעים מעל הספרות, כגון: $-!-@

3.4. רצוי שהסיסמא לא תכיל פרטים אישיים כגון: שם פרטי, שם משפחה, תאריך יום הולדת, מספר תעודת זהות, מספר חשבון בנק, רצף של מספרים וכדומה.

3.5. הקלדה שגויה של הסיסמא 5 פעמים ברציפות תגרום לחסימת השירות. במקרה כזה יהיה עליך לפנות לבנק לצורך שחרור סיסמתך.

3.6. מומלץ להימנע מלרשום את קוד המשתמש והסיסמא במקום גלוי, ובכל מקרה אין להחזיק רישום של קוד המשתמש והסיסמא יחד.

3.7. מומלץ לא להשתמש או להתקין תוכנה המאפשרת שמירת סיסמאות, באופן חלקי או מלא.

3.8. לידיעתך: הבנק ו/או מי מטעמו לא יבקש ממך את קוד המשתמש והסיסמא האישית לשירות ובכל מקרה אין לגלותה לאף אדם.

4. <u>שירות ותמיכה</u>

בכל שאלה, תקלה או בעיה, אנו עומדים לשירותך במוקד שירות הלקוחות של הבנק בטלפון: 02-5005303