# אתר און-ליין - אבטחת מידע

**הבנק רואה חשיבות רבה ומכרעת בנושא אבטחת פעילות הלקוחות בחשבונם.**

לפיכך, עושה הבנק מאמצים רבים לצורך הגנה על נתוני הלקוחות בכדי לאפשר פעילות מול מחשבי הבנק בגמישות מרבית תוך שימת דגש על היבטי אבטחת המידע השונים.

בכדי לאפשר לך ליהנות מגלישה נוחה ובטוחה, ריכזנו עבורך מספר המלצות והנחיות בנושא אבטחת מידע למשתמשים באתר "האון-ליין".

---

## המלצות והנחיות לשימוש במערכת

**כניסה לאתר הבנק ולאתר "האון ליין"**- לצורך גלישה לאתר הבנק יש להקליד את הכתובת המלאה של אתר הבנק: www.bankotsar.co.il לאחר קבלת דף הבית של האתר יש ללחוץ על קישור "כניסה לחשבון".

**לתשומת לבך**: **אין** להיכנס לאתר הבנק באמצעות קישורים המועברים אליך בדואר אלקטרוני.

**<u>אימות האתר</u>** במהלך הגלישה באתר יש לשים לב לאימות האתר כמפורט להלן:

- **כתובת האתר** - חשוב לוודא כי כתובת האתר מתחילה ב - online.bankotsar.co.il. למשך כל זמן ההתקשרות מול המערכת. בדקו כי לפני שורת הכתובת מופיע https:// המציין כי התקשורת מאובטחת ומוצפנת, או שמופיע מנעול סגור בצד שורת הכתובת.
- **צורה ומבנה** - יש לשים לב כי צורתו הכללית של האתר וחזותו החיצונית מוכרים לך.
- **הצפנת התקשורת** - חשוב לוודא כי בשורת הכתובת מופיע סמל של מנעול סגור (או מפתח שלם (בהתאם לגרסת הדפדפן המותקנת במחשבך)).
  סימן זה יופיע למשך כל זמן ההתקשרות מול המערכת. באמצעות לחיצה כפולה על המנעול/המפתח תוצג התעודה הדיגיטאלית שהונפקה לאתר. יש לוודא שהתעודה בתוקף והונפקה עבור בנק הבנק הבינלאומי הראשון לישראל בע"מ.
  במידה והאתר, צורתו והמבנה אינם תקינים, או שהתקשורת אינה מוצפנת, אין להזין את סיסמתכם ויש ליצור קשר מידי עם תמיכת האינטרנט בטלפון 03-5130038.

**<u>הזדהות</u>**

- הכניסה לאתר "האון ליין" מבוצעת באמצעות הקשת אמצעי הזיהוי, כפי שסופקו לך: קוד זיהוי משתמש וסיסמה אישית. נתונים אלו אישיים ואין להעבירם.
  מומלץ לוודא כי בעת ההזדהות שלך למערכת, לא ימצאו בסביבתך גורמים שאינם מורשים.
- אין למסור את אמצעי הזיהוי (כולל הסיסמה הראשונית) לאף גורם, גם אם הוא מזוהה עם הבנק (לתשומת ליבך נציגי הבנק לעולם **לא יפנו** בבקשת סיסמה מלקוחות). במידה ויבקשו ממך למסור את הסיסמה האישית, **אין** למסור אותה ויש לדווח על כך באופן מיידי לתמיכת האינטרנט בטלפון - 03-5130038 או במייל support@fibi.co.il.
- אין לשמור את אמצעי הזיהוי בקובץ במחשב.

**<u>סיסמאות</u>**

- **סיסמה ראשונית** - בכניסתך הראשונה לאתר ה"און ליין" תחויב להחליף את הסיסמה הראשונית אותה קיבלת מהסניף.
  סיסמה זו תקפה ל-30 יום בלבד ממועד קבלת דף הקוד. הסיסמה תבוטל אם לא תוחלף בתוך פרק זמן זה ויהיה עליך לפנות לסניפך לצורך הנפקת סיסמה חדשה.
- **בחירת סיסמה** - מומלץ להקפיד על בחירת סיסמה שתהיה קשה לניחוש המורכבת מצירוף של אותיות וספרות. יש להמנע משימוש בתאריכי לידה, שמות או נתונים אישיים אחרים אותם ניתן לגלות עליכם בקלות. כמו-כן, מומלץ ליצור סיסמה ייחודית לאתר הבנק ולא להשתמש באותה סיסמה המשמשת אתכם בכניסה לרשתות חברתיות ואתרים אחרים.
- **החלפת סיסמה** - המערכת מחייבת החלפת סיסמה מידי תקופה שתקבע ע"י הבנק. עם זאת ניתן להחליף סיסמה בכל עת. במידה ויש לך חשש כי לגורם נוסף ידועה הסיסמה שלך - יש להחליף מיידית את הסיסמה.
  החלפת הסיסמה תתבצע לאחר כניסה לאתר "האון ליין" תחת תפריט "שירותים" > "החלפת סיסמה".
- **חסימת סיסמה** – לאחר מספר ניסיונות של הקשת סיסמה שגויה, הכניסה למערכת תחסם. ניתן לבצע שחרור חסימה באופן עצמאי באמצעות האינטרנט, באופן הבא: לאחר קבלת דף הבית של האתר יש לבחור ב – "כניסה לחשבון" > "שכחת סיסמה/ נחסמה סיסמתך?".
  כמו כן, ניתן לפנות לתמיכת האינטרנט בטלפון 03-5130038, או במייל - support@fibi.co.il
- **שמירת סיסמה** - דפדפנים שונים עושים שימוש במנגנון לשמירת שם וסיסמת המשתמש. מומלץ לא להשתמש במנגנונים אלו באתר הבנק, ולבצע את הקלדת השם והסיסמה בכל כניסה לאתר הבנק.

**<u>מועד כניסה קודמת</u>** - בעת הכניסה לאתר "האון ליין" יצוין בראש הדף תאריך ושעת הכניסה הקודמים שלך למערכת.
מומלץ לוודא שהנתונים המוצגים אכן נכונים.

**<u>העברת אמצעי הזיהוי לגורם צד שלישי</u>** - אמצעי הזיהוי, כפי שסופקו לך הינם אישיים ואין להעבירם לאחר, מומלץ לא להעביר לגורם צד שלישי גם אם הוא פועל עבורך ומטעמך.

**<u>פעילות באתר</u>** - בעת השימוש באתר מומלץ לוודא שהנתונים המוצגים אכן נכונים, כי הפעילויות המפורטות אכן בוצעו על ידך. במידה וזיהית פעילות חריגה, יש לדווח לתמיכת האינטרנט בטלפון 03-5130038, או במייל - support@fibi.co.il.

**<u>סיום פעילות באתר ה"און ליין"</u>** - בעת סיום השימוש באתר "האון ליין", **יש לבצע יציאה מסודרת ע"י לחיצה על מקש "יציאה"**, הנמצא בחלקו העליון של המסך וסגירת הדפדפן.

**<u>PHISING - הונאה מקוונת</u>**

הונאה מקוונת הינה ניסיון לגניבת מידע רגיש ע"י התחזות ברשת האינטרנט. המידע הנגנב עלול להיות, בין היתר, אמצעי הזיהוי: קוד משתמש וסיסמאות, פרטי כרטיס אשראי, פרטי חשבון בנק ועוד.
התחזות יכולה להיעשות ע"י משלוח דואר אלקטרוני מגורם לגיטימי המבקש מכם פרטים אישיים. דרך נוספת לגניבת פרטים אישיים, היא ע"י בניית אתר מתחזה לאתר לגיטימי (למשל אתר מתחזה לאתר הבנק כאשר מטרתם לגרום למשתמש למסור את פרטיו האישיים. ברוב המקרים האתר המתחזה וכתובתו דומים מאוד לאתר המקורי אליו הם מתחזים והגורם שהפעיל את התרמית, ישתמש בנתונים שהועברו אליו בכדי לגנוב כסף או מידע.

**<u>אמצעי זיהוי Phishing</u>**

- הודעת דואר אלקטרוני מלווה בבקשה למענה מיידי ובהול שיכלול בקשה לקבלת פרטי זיהוי שלכם.
- הודעת דואר אלקטרוני המבקשת ללחוץ על קישור לדף אינטרנט/לכתובת אתר מתחזה הדומה לאתר אינטרנט המוכר לך.
- הודעת דואר אלקטרוני לא שגרתית, מגורם לא מוכר לכם, המלווה, לעיתים בשגיאות כתיב ובניסוח עילג.

**לתשומת לבך – הבנק אינו שולח בקשות לקבלת פרטים אישיים מהלקוחות באמצעות דואר אלקטרוני.**

**דרכי ההתגוננות הקיימים מפני Phishing**

- אין להעביר מידע אישי בדואר אלקטרוני ובודאי שלא במסגרת בקשה שאינה ביוזמתך.
- אין להיכנס לחשבון בנק באמצעות קישור המועבר דרך הודעת דואר אלקטרוני או הודעה במקום אחר – אלא באמצעות הקלדת כתובת האתר כמפורט בדף זה.
- היו חשדניים והיזהרו מהודעות המציעות מבצעים והנחות "חד פעמיים" "רק היום" "במיוחד בשבילך" וכד'.
- יש לשמור על סודיות הסיסמאות.
- הזנת פרטי דואר אלקטרוני תתבצע לאתרים מוכרים בלבד.
- אימות האתר כמפורט לעיל בהמלצות.
- קיבלתם הודעה המבקשת מכם להזין פרטי הזדהות, סיסמה או פרטי כרטיס אשראי? היא בוודאות לא מהבנק! אל תפתחו אותה, אל תענו לה והודיעו מייד למוקד תמיכת האינטרנט בטל 03-5130038, או במייל - support@fibi.co.il.

**<u>שמירת מידע במחשב האישי</u>** - באפשרות לשמור את דפי המידע בפורמטים שונים ( html, excel, pdf ועוד).

**לידיעתך - אבטחת המידע השמור במחשבך האישי הינו באחריותך והגישה למידע זה הינה על פי רמת האבטחה הקיימת במחשבך.**

## המלצות

**הכניסה לחשבון**

- מומלץ לא לגלוש לחשבון הבנק ממקומות ציבוריים.
- בכדי לבצע בקרה על הפעילות המבוצעת בחשבונכם, אנו ממליצים לבדוק, באופן שוטף, את הפעולות המבוצעות בחשבונותיכם השונים.

**המלצות כלליות**

- מומלץ להתקין תוכנת אנטי וירוס ולדאוג לעדכנה באופן שוטף.
- בצעו עדכונים שוטפים של מערכת ההפעלה, כולל ביצוע עדכוני אבטחת מידע, עפ"י המלצת יצרן מערכת ההפעלה.
- הימנעו מהורדת והתקנת קבצים ממקור בלתי ידוע.
- בזמן הגלישה באתר הבנק, הימנעו מכניסה לאתרים אחרים ומכניסה ל"חלונות קופצים".
- דאגו לבצע גיבויים בתדירות גבוהה, למידע אישי וחשוב השמור במחשבכם.
- מומלץ להתקין תוכנת Personal Firewall במחשבך האישי ולעדכנה על פי הצורך.
- מומלץ להתקין תוכנה לזיהוי תוכנות "ריגול" במחשבך האישי ולעדכנה על פי הצורך.

**תמיכה טכנית**

לבירורים, שאלות, תמיכה ובכל מקרה אחר בו מתעורר ספק בנושא אבטחת מידע, ניתן לפנות לתמיכת האינטרנט בטלפון 03-5130038, או במייל - support@fibi.co.il.

---

## אמצעי אבטחת המידע באתר ה"און ליין"

- הגישה למערכת הבנק מאובטחת ומבוקרת ע"י אמצעי אבטחה שונים, המאפשרים גישה רק לשירותים הנדרשים ע"י המערכת.
- המידע המשודר בין מחשב הבנק למחשב האישי שלך מוצפן.
- הבנק מפעיל אמצעי פיקוח ובקרה על ההתקשרות למערכת ומבצע, ניטור ובקרה על הפעילות המבוצעת במערכת.
- בדיקות אבטחת מידע של אתרי הבנק מבוצעות באופן שוטף על ידי מומחים בתחום אבטחת מידע.
- הגישה למערכת מתאפשרת רק לאחר הקשת אמצעי הזיהוי ; קוד משתמש וסיסמה. לאחר מספר ניסיונות של הקשת סיסמה שגויה, תופיע תמונת אימות למניעת נעילתך. הקשת סיסמה שגויה פעם נוספת תחסום את הכניסה למערכת.
- ניתוק אוטומטי של המערכת יבוצע לאחר פרק זמן ללא פעילות במערכת ותידרש הזדהות מחודשת.
- במידת הצורך יבוצע הפעלת שימוש באמצעי זיהוי נוסף של המשתמש.