גולשים בטוח

עדכוני אבטחה -

וודאו שמערכת ההפעלה, היישומים (אפליקציות/תוכנות) ותוכנת האנטי-וירוס המותקנים במכשיריכם מעודכנים בגרסתם האחרונה. גרסאות לא עדכניות חשופות יותר לפגיעויות מוכרות ומנוצלות ע"י גורמים זדוניים.

הטענה סלולרית מאובטחת -

הימנעו מהטענת מכשיריכם (סמארטפון/טאבלט) במקומות ציבוריים ובחיבורי USB אקראיים (עמדות הטענה מהירות בקניונים, נמלי תעופה, רכבות, אוטובוסים) שעלולה לגרום לגניבת מידע ממכשירכם. ניתן לרכוש מראש רכיב Data Blocker המאפשר הטענת המכשיר בראש שקט מבלי לחשוש שמידע יזלוג לגורם אחר.

גיבוי מידע -

הקפידו לגבות את המידע במכשיר. במקרה והמכשיר נגנב/נהרס/אבד, תוכלו לשחזר את המידע האחרון שנשמר. ניתן לגבות את המידע בשירותי ענן כדוגמת Google Drive, או על התקן USB חיצוני.

נקודה חמה -

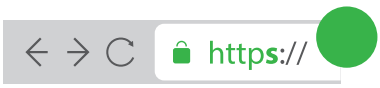
הגדירו סיסמה מאובטחת וחזקה לרשת ה - Wi Fi של הטלפון וכך תוכלו למנוע מגורמים שונים להתחבר ללא רשות.

בנק ירושלים
בנקאות משלימה

קונים חכם - קונים בטוח!

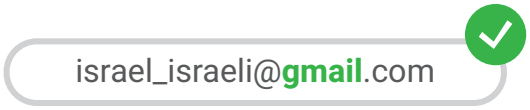
מוודאים כי האתר בטוח

כתובת האתר תקנית ונכונה
האתר מוצפן (https ומנעול)



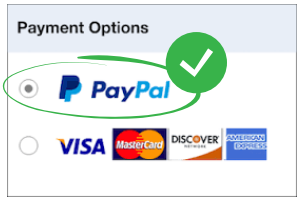
הרשמה לאתרי קניות

הירשמו באתרים עם כתובת דוא"ל אישית ולא ארגונית



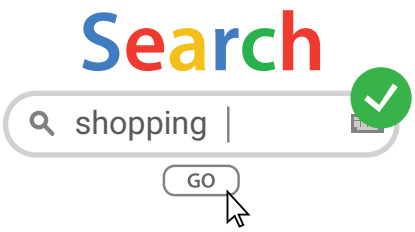
תשלום מאובטח באמצעות אפליקציות

העדיפו לרכוש באמצעות אפליקציות לתשלום מאובטח



לא לוחצים על קישורים

חפשו באופן יזום באתרים הרשמיים



היו זהירים וגלו חשד כלפי מבצעים "טובים מדי"

אם זה נשמע טוב מדי מכדי להיות אמיתי, זה חשוד

בנק ירושלים
בנקאות משלימה

נתפס ברשת

הודעות רבות שימצאו את דרכן אליכם יכילו
הצעות מפתות אם רק תלחצו על הקישור המצורף.
מומלץ להימנע מלחיצה על קישור בהודעות ולהגיע
לאתר המבוקש ביוזמתכם דרך חיפוש בגוגל.

סימנים מחשידים להונאה וטיפים למניעה:

קיבלתם הודעה בנוגע לחשבון הבנק?

נימת ההודעה דחופה או מופעל עליכם לחץ לבצע פעולה או להעביר מידע?

עצרו את הקליק על הקישור, בקשו לאמת את פרטי מבקש השירות ואם עולה לך חשש נוסף. תוכלו לאמת את הבקשה באמצעות שיחת טלפון ביוזמתכם למוקד הטלפוני של הבנק או כניסה מאובטחת לאתר הרשמי.

זכרו שגם אם על צג הטלפון מופיע מספר שנראה מוכר, יש אפשרות שהמספר מוסווה עקב שימוש באפליקציות זדוניות. בכל מקרה, אל תמסרו מידע אישי (כדוגמת קוד משתמש וסיסמה לחשבונכם). תוכלו לאמת את השיחה באמצעות תקשורת יזומה למוקד הטלפוני של הבנק או בגישה לאתר ולבנקאי.

הציגו לכם מסמכים או תעודות כביכול רשמיות? זו אינה אינדיקציה לאמינות השיחה. העבירו לבדיקת הבנקאי שלכם.

זכרו כי דיוג (פישינג) יכול להתבצע בכל תוכנת העברת מסרים-

ואפילו בשיחת טלפון

אתה הכי חזק
שהסיסמה שלך חזקה

סיסמה מורכבת וארוכה

ככל שהסיסמה ארוכה יותר כך יהיה קשה יותר לפצח אותה.
מומלץ ליישם סיסמה בעלת אורך של 8 תווים ומעלה.
תוכן הסיסמה מורכב מתווים מסוגים שונים כמו אותיות גדולות, אותיות קטנות וסימנים מיוחדים.

חשוב לאבטח את מכשיריכם -
הגדירו סיסמת כניסה למכשיר (סלולר/טאבלט/מחשב נייד) כדי למנוע גישה של גורם בלתי מורשה.

אימות דו-שלבי (2FA) -
הפעילו שירות אימות דו-שלבי להגנה נוספת על חשבונותיכם האישיים. במקרה בו גורם זדוני השיג את פרטי הזיהוי שלכם לחשבון, הוא לא יוכל להשלים את פעולת ההשתלטות על החשבון ללא קבלת הקוד האימות הנשלח למספר הנייד שלכם.

בכל מקרה שבו מתעורר חשד לשימוש לא מורשה בחשבון שלך או חשד לגניבת פרטי זיהוי לאתר, אובדן מכשיר טלפון, גניבת מכשיר, שימוש לרעה במכשיר או החלפת מספר טלפון, יש להודיע על כך לבנק באופן מיידי באמצעות ערוץ התקשורת הנוח לך:

טלפון לנציג בנק ירושלים - 5727*

טלפון למוקד התמיכה הטכנית – 076-8096666

בנק ירושלים
בנקאות משלימה